

# Integration Guide

version 1.7

STS PayOne

21 April 2020

## PROPRIETARY INFORMATION

STS PayOne and the STS PayOne logo are registered trademarks of STS Payment Network DMCC. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or the names of their products. STS PayOne disclaims proprietary interest in the marks and names of others.

The information in this document has been reviewed and is believed to be accurate. However, neither STS PayOne nor its affiliates assume any responsibility for inaccuracies, errors, or omissions that may be contained herein. In no event will STS PayOne or its affiliates be liable for direct, indirect, special, incidental, or consequential damages resulting from any defect or omission in this document, even if advised of the possibility of such damages.

STS PayOne reserves the right to make improvements or changes to this document and information contained within, and to the products and services described at any time, without notice or obligation.

STS PayOne understands that any award to supply the products/ provide the services that are the subject of this document are subject to the mutual execution of a definitive written agreement.

All information supplied for the purpose of this document is to be considered STS PayOne confidential.

© 2016 STS PayOne

# 1 Contents

<b>1. INTRODUCTION</b>	<b>6</b>
1.1. WHO SHOULD READ THIS DOCUMENT?	6
1.2. PURPOSE	6
1.3. PREREQUISITES	6
<b>2. OVERVIEW</b>	<b>7</b>
2.1. AUTHENTICATION TOKEN	7
2.2. COMMUNICATION MODEL	8
2.3. TRANSACTION FLOW	9
2.4. HOW TO START	10
2.5. TOKENIZATION	11
<b>3. SMARTROUTE MESSAGES</b>	<b>12</b>
3.1. REDIRECT PAYMENT – REDIRECT PRE-AUTHORIZATION MESSAGE	12
3.1.1. REQUEST FIELDS: BASIC FIELDS	12
3.1.2. RESPONSE FIELDS: BASIC FIELDS	13
3.1.3. OTHER OPTIONAL FIELDS	15
3.2. DIRECT POST PAYMENT – DIRECT POST PRE-AUTHORIZATION MESSAGE	18
3.2.1. REQUEST FIELDS: BASIC FIELDS	18
3.2.2. RESPONSE FIELDS: BASIC FIELDS	20
3.2.3. OTHER OPTIONAL FIELDS	22
3.3. DIRECT POST VERIFY MESSAGE	25
3.3.1. REQUEST FIELDS: BASIC FIELDS	25
3.3.2. RESPONSE FIELDS: BASIC FIELDS	27
3.3.3. OTHER OPTIONAL FIELDS	29
3.4. API PAYMENT – API PRE-AUTHORIZATION	31
3.4.1. REQUEST FIELDS: BASIC FIELDS	32
3.4.2. RESPONSE FIELDS: BASIC FIELDS	34
3.4.3. OTHER OPTIONAL FIELDS	37
3.5. API mPAYMENT	39
3.5.1. REQUEST FIELDS: BASIC FIELDS	39
3.5.2. RESPONSE FIELDS: BASIC FIELDS	42
3.5.3. OTHER OPTIONAL FIELDS	44
3.6. API APPROVE	46
3.6.1. REQUEST FIELDS: BASIC FIELDS	46
3.6.2. RESPONSE FIELDS: BASIC FIELDS	48
3.6.3. OTHER OPTIONAL FIELDS	49
3.7. INQUIRY MESSAGE	50
3.7.1. REQUEST FIELDS	50
3.7.2. RESPONSE FIELDS	51
3.8. REFUND MESSAGE	54
3.8.1. REQUEST FIELDS	54
3.8.2. RESPONSE FIELDS	55
3.9. RECURRING PAYMENT	57
3.9.1. REQUEST FIELDS: BASIC FIELDS	57
3.9.2. RESPONSE FIELDS: BASIC FIELDS	59

3.9.3. OTHER OPTIONAL FIELDS -----	60
3.10. COMPLETION MESSAGE -----	63
3.10.1. REQUEST FIELDS -----	63
3.10.2. RESPONSE FIELDS -----	64

## 4. APPENDICES-----66

4.1. APPENDIX A: RESPONSE CODES -----	66
4.1.1. REDIRECT PAYMENT RESPONSE CODES -----	66
4.1.2. DIRECT POST PAYMENT RESPONSE CODES -----	68
4.1.3. DIRECT POST VERIFY RESPONSE CODES -----	71
4.1.4. API PAYMENT RESPONSE CODES -----	74
4.1.5. API MPAYMENT RESPONSE CODES -----	76
4.1.6. API APPROVE RESPONSE CODES -----	79
4.1.7. TRANSACTION INQUIRY RESPONSE CODES -----	80
4.1.8. REFUND RESPONSE CODES -----	81
4.1.9. RECURRING PAYMENT RESPONSE CODES -----	83
4.2. APPENDIX B: SECURE HASH -----	86
4.2.1. REDIRECT PAYMENT -----	86
4.2.2. DIRECT POST PAYMENT -----	88
4.2.3. DIRECT POST VERIFY -----	90
4.2.4. API PAYMENT -----	92
4.2.5. API MPAYMENT -----	94
4.2.6. API APPROVE -----	96
4.2.7. TRANSACTION INQUIRY -----	98
4.2.8. REFUND TRANSACTION -----	100
4.2.9. RECURRING PAYMENT -----	102
4.2.10. COMPLETION TRANSACTION -----	104
4.3. APPENDIX C: UPDATE NOTIFICATION MESSAGE -----	106
4.3.1. RESPONSE FIELDS: BASIC FIELDS -----	106
4.3.2. OTHER OPTIONAL FIELDS -----	107
4.4. APPENDIX D: 3D-SECURE IMPLEMENTATION -----	109
4.5. APPENDIX E: SADAD IMPLEMENTATION -----	113

TABLE 1: REDIRECT PAYMENT RESPONSE CODES -----	66
TABLE 2 : DIRECT POST (SALE) RESPONSE CODES -----	68
TABLE 3 DIRECT POST VERIFY RESPONSE CODES -----	71
TABLE 4 : API PAYMENT RESPONSE CODES -----	74
TABLE 5 : API MPAYMENT RESPONSE CODES -----	76
TABLE 6 : API APPROVE RESPONSE CODES -----	79
TABLE 7: TRANSACTION INQUIRY RESPONSE CODES -----	80
TABLE 8: REFUND RESPONSE CODES -----	81
TABLE 9 : RECURRING PAYMENT RESPONSE CODES -----	83
TABLE 10: REDIRECT PAYMENT – REQUEST MESSAGE -----	86
TABLE 11 REDIRECT PAYMENT – RESPONSE MESSAGE -----	87
TABLE 12 DIRECT POST PAYMENT – REQUEST MESSAGE -----	88
TABLE 13: DIRECT POST PAYMENT – RESPONSE MESSAGE -----	89
TABLE 14 DIRECT POST VERIFY – REQUEST MESSAGE -----	90
TABLE 15 DIRECT POST VERIFY – RESPONSE MESSAGE -----	91

TABLE 16 API PAYMENT – REQUEST MESSAGE ----- 92

TABLE 17 API PAYMENT – RESPONSE MESSAGE----- 93

TABLE 18 API MPAYMENT – REQUEST MESSAGE----- 94

TABLE 19 API MPAYMENT – RESPONSE MESSAGE ----- 95

TABLE 20 API APPROVE – REQUEST MESSAGE ----- 96

TABLE 21 API APPROVE – RESPONSE MESSAGE ----- 97

TABLE 22 TRANSACTION INQUIRY - REQUEST MESSAGE----- 98

TABLE 23 TRANSACTION INQUIRY - RESPONSE MESSAGE ----- 99

TABLE 24 REFUND TRANSACTION - REQUEST MESSAGE----- 100

TABLE 25 REFUND TRANSACTION - RESPONSE MESSAGE ----- 101

TABLE 26 RECURRING PAYMENT – REQUEST MESSAGE ----- 102

TABLE 27 RECURRING PAYMENT – RESPONSE MESSAGE ----- 103

TABLE 28 COMPLETION TRANSACTION - REQUEST MESSAGE ----- 104

TABLE 29 COMPLETION TRANSACTION - RESPONSE MESSAGE----- 105

# 1. Introduction

## 1.1. Who should read this document?

This document is intended for merchant system designer and developer planning to integrate with SmartRoute interface to perform e-Commerce. Readers of this document should be web application developers.

## 1.2. Purpose

This guide is written for merchants who have signed up through SmartRoute system to use it as their Integration point with Payment Gateways for handling electronic transactions (payment, refund, confirm.. etc.) and from different payment methods (credit card, debit card...etc.), by using the HTTPS Post as programming interface to perform the transactions. In particular, it describes the format for sending transactions and the corresponding received responses.

## 1.3. Prerequisites

- Merchant is contracted with Payment Gateway as an e-Commerce Merchant.
- Merchant is contracted with SmartRoute as an Integration point with the Payment Gateways.
- Merchant is provided with a SmartRoute profile to generate Authentication Token used for integration.
- Merchant has a profile at Payment Gateway side.

## 2. Overview

SmartRoute is the connecting link between the Merchant and the Payment Gateways, it acts as a smart dynamic router that captures the card number, in case of card payment, determines the best payment gateway for the transaction based on defined business rules then forwards the transaction to the selected gateway to be processed.

So via a single integration with SmartRoute System, the merchant will have the capabilities of various payment gateways to process its transactions with the best possible rates.

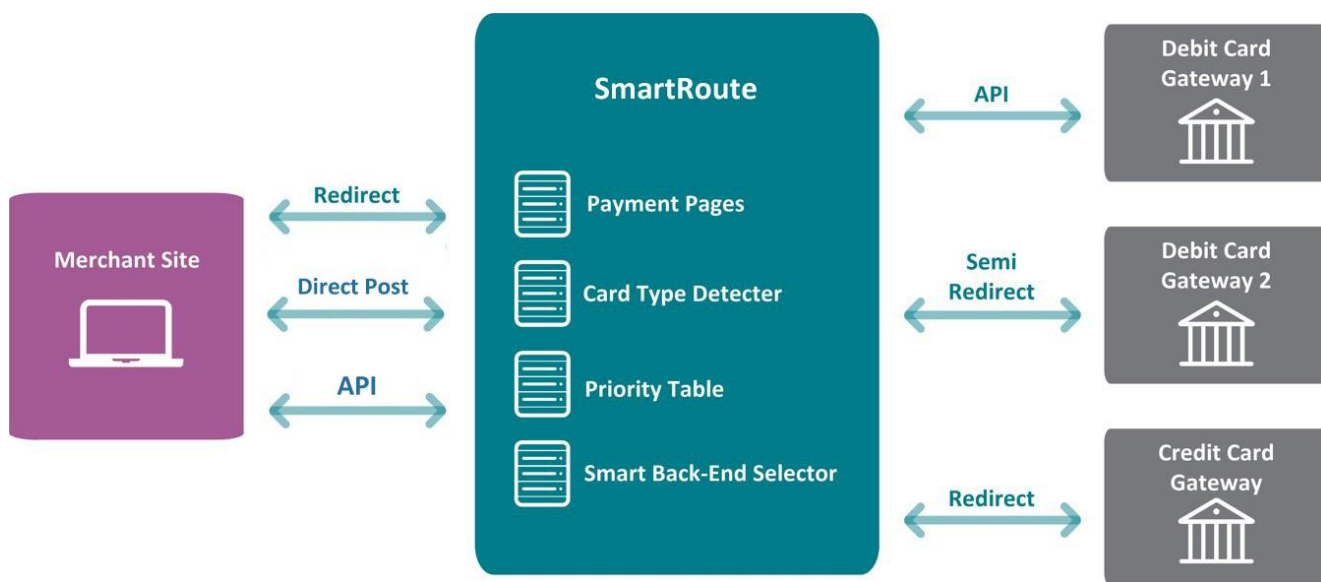


Figure 1: Conceptual Solution Diagram

Merchant interacts with SmartRoute to perform electronic transactions through a secure channel. Merchant constructs the request which consists of pre-defined fields and their values. Then sends the request and processes the received response from SmartRoute system.

### 2.1. Authentication Token

#### Data Integrity

To guarantee request/response data integrity a Secure Hash will be generated for each message, this Secure Hash will be created using all message fields.

Upon receiving a request/response message the receiver will recreate the Secure Hash from received message parameters and compare it with Secure Hash already sent within the message.

#### Authentication

For each Merchant an Authentication Token will be generated/ set. This Authentication Token is used as part of the Secure Hash value and will only be known to Merchant application and SmartRoute. Accordingly message recipient (Merchant or SmartRoute) will include Authentication Token value when generating the Secure Hash value.

**Merchant must make sure to:**

- Store the Authentication Token in a secure place as a secure database or file.
- Not store the Authentication Token within the source code of an ASP, JSP or any web page standing the chance of being accessed or viewed via web.

## **2.2. Communication Model**

Interacting with SmartRoute system can be done via three types of communication models based on message type. The communication models are:

- **Redirection communication model:** in this model Merchant site issues Http redirection command to customer (card holder) browser; customer gets redirected to SmartRoute system site where the customer is requested to provide some input to complete the cycle. After conducting the payment, SmartRoute system redirects the customer back to the merchant site based on a predefined merchant's URL.
- **Direct Post communication model:** in this model, the Merchant will be able to fully maintain the payment process without having to handle and store sensitive payment data. The site passes the sensitive data entered by the customer using Http redirection to SmartRoute system without going through the merchant's server. The merchant will have to prepare the request parameters along with their corresponding secure hash in the form specified in ([Appendix B: Secure Hash - Direct Post Payment](#)) which will be submitted to SmartRoute without including the sensitive data in the secure hash.

The customer is not requested to provide any input to complete the cycle as all the inputs are already passed by the merchant site. After conducting the payment, SmartRoute system redirects the customer back to the merchant site based on a predefined merchant's URL.

Note: Sensitive data is:

- In case of a Card Payment: Card Number, Cardholder Name, Expiry Date and Security Code.
- In case of a SADAD Payment: SADAD OLP ID

**API Model:** in this model Merchant site collects all the needed information from customer (card holder) and sends Https POST call from merchant side to SmartRoute system (without using the customer browser). SmartRoute system processes the request and gets back to the merchant with response. Therefore, the merchant system can process the received response.

## 2.3. Transaction Flow

### Request Flow

- Merchant prepares request message which includes request's fields based on the message ID (i.e. Sale, Inquiry Status ... etc.)
- Merchant generates Secure Hash using request parameters and Authentication Token value
- Merchant sends the request including the Secure Hash to SmartRoute.
- SmartRoute System upon receiving the request will retrieve Authentication Token value stored for this merchant at SmartRoute side.
- SmartRoute System Regenerates Secure Hash using received request parameters and Authentication Token stored at SmartRoute System.
- SmartRoute compares generated Secure Hash with received Secure Hash, if values mismatch, request will be rejected. Else SmartRoute will continue processing request.

### Response Flow

- SmartRoute System prepares response for merchant request.
- SmartRoute System generates Secure Hash using response parameters and Authentication Token stored at SmartRoute side.
- SmartRoute sends the response including the Secure Hash to Merchant.
- Merchant upon receiving the response will use response parameter and Authentication Token value stored at Merchant application to regenerate Secure Hash for response
- Merchant compares generated Secure Hash with received Secure Hash, if values mismatch. Response will be rejected. Else Merchant application will continue processing response

### Note:

The merchant can arrange with SmartRoute's Support Team to include extra parameters (dynamic fields) in the messages' requests/responses if the need arises. These dynamic fields must be included in the secure hash generation.

## 2.4. How to Start

Merchants integrating with SmartRoute have the flexibility of choosing the needed messages to conduct their transactions from a varied selection of messages based on their platform (e.g. Native Mobile App or a Web Application) and their preferred communication model (*upon arrangement with the SmartRoute's Support Team*), as follows:

- If the merchant is integrating a **Web Application** and needs to have full control of the payment details capturing process, then the following messages must be considered in the integration:
  - **API Payment**: This message is used to perform a payment.
  - **API Pre-Auth**: This message is used to perform a Pre-Authorization Transaction.
  - **API Approve**: Complement message and not to be used alone. Used to finalize some API Payment transactions.
  - **Refund**: This message is used to refund a transaction.
  - **Inquiry**: This message is used to inquire about the status of a transaction.
  - **Completion**: This message is used complete a Pre-Authorization Transaction.
- If the merchant is integrating a native **Mobile Application** and needs to have full control of the payment details capturing process, then the following messages must be considered in the integration:
  - **API mPayment**: This message is used to perform a payment.
  - **API Approve**: Complement message and not to be used alone. Used to finalize some API mPayment transactions.
  - **Refund**: This message is used to refund a transaction.
  - **Inquiry**: This message is used to inquire about the status of a transaction.
- If the merchant is integrating a **Web Application** and needs SmartRoute to handle the **entire** payment details capturing process without any capturing at the merchant side, then the following messages must be considered in the integration:
  - **Redirect Payment**: This message is used to perform a payment.
  - **Redirect Pre-Authorization**: This message is used to perform a Pre-Authorization.
  - **Refund**: This message is used to refund a transaction.
  - **Inquiry**: This message is used to inquire about the status of a transaction.
  - **Update Notification**: This message is used to notify the merchant of the status of the transaction. It is useful if the customer closed the browser before being redirected back to the merchant site.
  - **Completion**: This message is used complete a Pre-Authorization Transaction.
- If the merchant is integrating a **Web Application** and needs to be in control of the design and hosting of the payment page which posts silently to SmartRoute directly from the customer's browser, then the following messages must be considered in the integration:
  - **Direct Post Payment**: This message is used to perform a payment
  - **Redirect Pre-Authorization**: This message is used to perform a Pre-Authorization
  - **Refund**: This message is used to refund a transaction.
  - **Inquiry**: This message is used to inquire about the status of a transaction.

- **Update Notification:** This message is used to notify the merchant of the status of the transaction. It is useful if the customer closed the browser before being redirected back to the merchant site.
- **Completion:** This message is used complete a Pre-Authorization Transaction.

## 2.5. Tokenization

Merchants integrating with SmartRoute can use the tokenization feature, which enables the merchant to send a token to represent the card number, card expiry date, and card holder name in order to enhance security. In order to use it, there are some specific parameters:

- GenerateToken
- Token
- Response.Token

However, using those parameters should meet some conditions:

- You cannot send a token with card details (card number, card expiry date, card holder name, security code), as this will lead to an error, you can either send card details or a token.
- You cannot request to generate a token while sending a token, and this will lead to an error.

## 3. SmartRoute Messages

### 3.1. Redirect Payment – Redirect Pre-Authorization Message

This message is intended to perform a payment using SmartRoute interface. It's based on the Redirection communication model as described in [Communication Model](#) section.

Two types of Redirect Payments can be used in SmartRoute:

- Redirect Payment
- Redirect Pre-Authorization

#### 3.1.1. Request Fields: Basic Fields

Field Name				
Field Description				
Request/Response	Required/Optional	Field Type	Length	Sample Data

MessageID				
Alphanumeric value representing the action to be called: <ul style="list-style-type: none"><li>• 1 for Redirect Payment</li><li>• 6 for Redirect Pre-Authorization</li></ul>				
Request	Required	Alphanumeric	2	1

TransactionID				
The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				
Request	Required	Alphanumeric	20	1440954863817

MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Request	Required	Alphanumeric	40	MID0001

Amount				
A numeric value containing the Item purchase amount ISO Formatted with no decimal point.  e.g. 100 for 1.00 USD				
Request	Required	Numeric	9	100

CurrencyISOCode				
The numeric ISO Code for the currency and not the character value.  e.g. 840 for US Dollar 400 for JOD 682 for SAR 784 for AED				
Request	Required	Numeric	3	840

PaymentDescription				
Alphanumeric string containing a narrative description of the payment order using the language specified in the language parameter. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Request	Required	Alphanumeric	100	SamplePayment

SecureHash				
Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all parameters (required parameters and optional parameters if they are provided) ordered alphabetically by parameter's name should be part of the secure hash, with no separators and no terminating character. Please refer to <a href="#">Appendix B: Secure Hash – Redirect Payment</a> for more details about secure hash generation				
Request	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e

### 3.1.2. Response Fields: Basic Fields

Response.StatusCode				
Alphanumeric value representing the response code, this code covers errors generated by SmartRoute. Check <a href="#">Appendix A: Redirect Payment Response Codes</a> for descriptive details about Response Codes.				
Response	Required	Alphanumeric	5	00000

Response.StatusDescription				
Alphanumeric value representing a message describing the response status as received from SmartRoute using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Response	Required	Alphanumeric	100	Payment processed successfully

Response.Amount				
A numeric value containing the total transaction amount ISO Formatted with no decimal point.				

e.g. 1.00 USD received as 100 1.00 SAR received as 100 1.00 AED received as 100 1.000 JOD received as 1000				
Response	Required	Numeric	9	100

Response.CurrencyISOCode				
The numeric ISO Code for the currency and not the character value.  e.g. 840 for US Dollar 400 for JOD 682 for SAR 784 for AED				
Response	Required	Numeric	3	840

Response.MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Response	Required	Alphanumeric	40	MID0001

Response.TransactionID				
The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				
Response	Required	Alphanumeric	20	201508180000001

Response.MessageID				
Alphanumeric value representing the called action: <ul style="list-style-type: none"> <li>1 For Redirect Payment</li> <li>6 For Redirect Pre-Authorization</li> </ul>				
Response	Required	Alphanumeric	2	1

Response.SecureHash				
Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all response parameter appended in alphabetical order based on parameter's name, with no separators and no terminating character. Please refer to <u>Appendix B: Secure Hash – Redirect Payment</u> for more details about secure hash generation.				
Response	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e

### 3.1.3. Other Optional Fields

Language				
Alphabetic value representing the language of the interface displayed to customer at merchant site, and used as language for the payment description parameter. PG will use this value to display the interface supporting selected language to the customer during the payment process. Supported values are: En Ar				
Request	Optional	Alphanumeric	2	En

ItemID				
The custom item ID for the merchant.				
Request	Optional	Alphanumeric	25	Item1

ThemeID				
The custom theme ID for the merchant.				
Request	Optional	Alphanumeric	40	Theme1

Version				
A numeric value with (.) separator representing the version of the command to be used. Send it as 1.0. Send it as 2.0 to: 1- Add Response.PaymentMethod to Response Fields. 2- Use the RecurringSeriesID field.				
Request	Optional	Numeric	5	1.0

ResponseBackURL				
Merchant site response page URL that will receive the response from SmartRoute, this can help merchant having different response pages based on the requested service or any other criteria				
Request	Optional	Alphanumeric	512	<a href="https://MerchantReplyURL/PaymentReply.do">https://MerchantReplyURL/PaymentReply.do</a>

Channel				
The Channel to be used by SmartRoute System. It could be one of: 0 → E-Commerce, 1 → IVR 2 → POS				
Request	Optional	Numeric	1	0

Quantity				
A numeric value greater than ZERO represents the quantity of purchased Item				
Request	Optional	Numeric	5	1

GenerateToken				
---------------	--	--	--	--

This flag indicates whether to generate a token for the entered card information or not. It accepts the values "Yes" and "No". Sending this field as "No" acts like when the field is not sent at all. This parameter is a part of the tokenization parameters, check the [Tokenization](#) section for more details.

Request	Optional	Alphabetic	3	Yes
---------	----------	------------	---	-----

#### Token

The token that will be used in this request; to represent a previously used card information. This parameter is a part of the tokenization parameters, check the [Tokenization](#) section for more details.

Request	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27
---------	----------	--------------	----	--

#### RecurringSeriesID

The series id that will be used in this request; to represent the card number that will be used in this transaction. The same value should be provided when performing a recurring payment.

This field is supported only if the Version field is set to 2.0

Request	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27
---------	----------	--------------	----	--

#### Response.CardExpiryDate

Expiry date of the card (MMYY).

Response	Optional	Alphanumeric	4	0416
----------	----------	--------------	---	------

#### Response.CardHolderName

Card Holder Name

Response	Optional	Alphanumeric	32	FName LName
----------	----------	--------------	----	-------------

#### Response.CardNumber

Masked Card Number

Response	Optional	Alphanumeric	19	4747*****123
----------	----------	--------------	----	--------------

#### Response.GatewayStatusCode

Alphanumeric value representing the gateway response code, this code covers errors generated by the chosen gateway.

Response	Optional	Alphanumeric	15	0000
----------	----------	--------------	----	------

#### Response.GatewayStatusDescription

Alphanumeric value representing a message describing the response status as received from the chosen gateway using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Response	Optional	Alphanumeric	100	Sample Gateway Description

<b>Response.GatewayName</b>				
This value represents the gateway name that processed the transaction, it can be alphanumeric with some special characters like space, '@' and '_ '.				
Response	Optional	Alphanumeric and Some Special	40	TestGateway

<b>Response.RRN</b>				
Alphanumeric value representing a Receipt Reference Number as a reference for the current payment transaction. This value will be returned if the value is provided from the gateway.				
Response	Optional	Alphanumeric	60	2015082016004628400000000000

<b>Response.ApprovalCode</b>				
Approval Code received from Payment Processor such as Visa. It will be return only when the transaction is success. This value will be returned if the value is provided from the gateway.				
Response	Optional	Alphanumeric	10	12345678

<b>Response.Token</b>				
The token that is assigned to the entered card information; responding to a "GenerateToken" flag with the value "Yes". This parameter is a part of the tokenization parameters, check the <a href="#">Tokenization</a> section for more details.				
Response	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27

<b>Response.PaymentMethod</b>				
An Alphanumeric value to indicate which payment method will be used. Supported values depend on the requested <b>version</b> as follows: <b>If Version is 1.0 :</b> <b>1 →</b> that means a payment using Card. <b>2 →</b> that means a payment using SADAD.  <b>If Version is 2.0 :</b> <b>1:Card Name</b> (1 indicates Payment Method Card) e.g. <b>1:Visa</b> <b>2</b> (indicates Payment Method SADAD).  * Possible Card Names are provided by SmartRoute operation team upon merchant enrollment.				
Request	Conditional	Alphanumeric	42	2

### 3.2. Direct Post Payment – Direct Post Pre-Authorization Message

This message is intended to perform a payment using the merchant's interface. It's based on the Direct Post communication model as described in [Communication Model section](#).

Two types of Direct Post Payments can be used in SmartRoute:

- Direct Post Payment
- Direct Post Pre-Authorization

#### 3.2.1. Request Fields: Basic Fields

Field Name				
Field Description				
Request/Response	Required/Optional	Field Type	Length	Sample Data

MessageID				
Alphanumeric value representing the action to be called: <ul style="list-style-type: none"><li>• 1 for Direct Post Payment</li><li>• 6 for Direct Post Pre-Authorization</li></ul>				
Request	Required	Alphanumeric	2	1

TransactionID				
The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				
Request	Required	Alphanumeric	20	1440954863817

MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Request	Required	Alphanumeric	40	MID0001

Amount				
A numeric value containing the Item purchase amount ISO Formatted with no decimal point.  e.g. 100 for 1.00 USD				
Request	Required	Numeric	9	100

CurrencyISOCode				
The numeric ISO Code for the currency and not the character value.  e.g. 840 for US Dollar				

400 for JOD 682 for SAR 784 for AED				
Request	Required	Numeric	3	840

<b>PaymentMethod</b>				
A numeric value to indicate which payment method will be used. Supported values are: 1 → which means a payment using Card. 2 → which means a payment using SADAD.				
Request	Required	Numeric	1	2

<b>CardNumber</b>				
The customer's card number that will be used in the payment. This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
<b>Note: Shouldn't be included in the Secure Hash</b>				
Request	Conditional	Numeric	19	4111111111111111

<b>ExpiryDateYear</b>				
The customer's card expiry date year digits that will be used in the payment. The format of this parameter should be in the form (YY). This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
<b>Note: Shouldn't be included in the Secure Hash</b>				
Request	Conditional	Numeric	2	17

<b>ExpiryDateMonth</b>				
The customer's card expiry date month digits that will be used in the payment. The format of this parameter should be in the form (MM). This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
<b>Note: Shouldn't be included in the Secure Hash</b>				
Request	Conditional	Numeric	2	02

<b>SecurityCode</b>				
The customer's card Security Code (e.g. CVV or CVC) depending on the Card Type that will be used in the payment. This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
<b>Note: Shouldn't be included in the Secure Hash</b>				
Request	Conditional	Numeric	4	123

<b>CardHolderName</b>				
-----------------------	--	--	--	--

The customer's card holder name that will be used in the payment. This parameter is optional if the sent <b>PaymentMethod</b> parameter is 1 (Card). The format should be alphabetic with spaces allowed.				
<b>Note: Shouldn't be included in the Secure Hash</b>				
Request	Optional	Alphabetic	64	Card Holder Name

<b>PaymentDescription</b>				
Alphanumeric string containing a narrative description of the payment order using the language specified in the language parameter.				
Request	Required	Alphanumeric	100	SamplePayment

<b>SadadOlpId</b>				
The customer's SADAD OLP ID that will be used in the payment. This parameter is required if the sent <b>PaymentMethod</b> parameter is 2 (SADAD).				
<b>Note: Shouldn't be included in the Secure Hash</b>				
Request	Conditional	Alphanumeric	12	Test123

<b>SecureHash</b>				
Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all parameters(required parameters and optional parameters if they are provided) except ( <b>CardNumber, SecurityCode, CardHolderName, ExpiryDateYear, ExpiryDateMonth, SadadOlpId</b> since those parameters are entered by the customer (card holder) on the screen, and will be submitted directly to SmartRoute's URL, so they can't be captured and entered in the secure hash parameters.) Ordered alphabetically by parameter's name should be part of the secure hash, with no separators and no terminating character. Please refer to <a href="#">Appendix B: Secure Hash – Direct Post Payment</a> for more details about secure hash generation				
Request	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e

### 3.2.2. Response Fields: Basic Fields

<b>Response.StatusCode</b>				
Alphanumeric value representing the response code, this code covers errors generated by SmartRoute. Check <a href="#">Appendix A: Direct Post Payment Response Codes</a> for descriptive details about Response Codes.				
Response	Required	Alphanumeric	5	00000

Response.StatusDescription				
Alphanumeric value representing a message describing the response status as received from SmartRoute using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Response	Required	Alphanumeric	100	Payment processed successfully

Response.Amount				
A numeric value containing the total transaction amount ISO Formatted with no decimal point.  e.g. 1.00 USD received as 100 1.00 SAR received as 100 1.00 AED received as 100 1.000 JOD received as 1000				
Response	Required	Numeric	9	100

Response.CurrencyISOCode				
The numeric ISO Code for the currency and not the character value.  e.g. 840 for US Dollar 400 for JOD 682 for SAR 784 for AED				
Response	Required	Numeric	3	840

Response.MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Response	Required	Alphanumeric	40	MID0001

Response.TransactionID				
The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				
Response	Required	Alphanumeric	20	201508180000001

Response.MessageID				
Alphanumeric value representing the action to be called, 1 for Sale				
Response	Required	Alphanumeric	2	1

Response.SecureHash				
Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all response parameter appended in alphabetical order based on parameter's name, with no separators and no terminating character. Please refer to <u>Appendix B: Secure Hash – Direct Post (Sale)</u> for more details about secure hash generation.				
Response	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e

### 3.2.3. Other Optional Fields

Language				
Alphabetic value representing the language of the interface displayed to customer at merchant site, and used as language for the payment description parameter. PG will use this value to display the interface supporting selected language to the customer during the payment process. Supported values are: En Ar				
Request	Optional	Alphanumeric	2	En

ItemID				
The custom item ID for the merchant.				
Request	Optional	Alphanumeric	25	Item1

Version				
A numeric value with (.) separator representing the version of the command to be used. Send it as 1.0. Send it as 2.0 to: 1- Add Response.PaymentMethod to Response Fields. 2- Use the RecurringSeriesID field.				
Request	Optional	Numeric	5	1.0

Channel				
The Channel to be used by SmartRoute System. It could be one of: 0 → E-Commerce, 1 → IVR 2 → POS				
Request	Optional	Numeric	1	0

Quantity				
A numeric value greater than ZERO represents the quantity of purchased Item				
Request	Optional	Numeric	5	1

ResponseBackURL				
Merchant site response page URL that will receive the response from SmartRoute, this can help merchant having different response pages based on the requested service or any other criteria				
Request	Optional	Alphanumeric	512	https://MerchantReplyURL/PaymentReply.do

GenerateToken				
This flag indicates whether to generate a token for the sent card information or not. It accepts the values "Yes" and "No". Sending this field as "No" acts like when the field is not sent at all. This parameter is a part of the tokenization parameters, check the <a href="#">Tokenization</a> section for more details.				
Request	Optional	Alphabetic	3	Yes

Token				
The token that will be used in this request; to represent a previously used card information. This parameter is a part of the tokenization parameters, check the <a href="#">Tokenization</a> section for more details.				
Request	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27

RecurringSeriesID				
The series id that will be used in this request; to represent the card number that will be used in this transaction. The same value should be provided when performing a recurring payment.				
This field is supported only if the Version field is set to 2.0				
Request	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27

Response.CardExpiryDate				
Expiry date of the card (MMYY).				
Response	Optional	Alphanumeric	4	0416

Response.CardHolderName				
Card Holder Name				
Response	Optional	Alphanumeric	32	FName LName

Response.CardNumber				
Masked Card Number				
Response	Optional	Alphanumeric	19	4747*****123

Response.GatewayStatusCode				
Alphanumeric value representing the gateway response code, this code covers errors generated by the chosen gateway.				

Response	Optional	Alphanumeric	15	0000
----------	----------	--------------	----	------

#### Response.GatewayStatusDescription

Alphanumeric value representing a message describing the response status as received from the chosen gateway using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.

Response	Optional	Alphanumeric	100	Sample Gateway Description
----------	----------	--------------	-----	----------------------------

#### Response.GatewayName

This value represents the gateway name that processed the transaction, it can be alphanumeric with some special characters like space, '@' and '\_'.

Response	Optional	Alphanumeric and Some Special	40	TestGateway
----------	----------	-------------------------------	----	-------------

#### Response.RRN

Alphanumeric value representing a Receipt Reference Number as a reference for the current payment transaction. This value will be returned if the value is provided from the gateway.

Response	Optional	Alphanumeric	60	2015082016004628400000000000
----------	----------	--------------	----	------------------------------

#### Response.ApprovalCode

Approval Code received from Payment Processor such as Visa. It will be returned only when the transaction is success. This value will be returned if the value is provided from the gateway.

Response	Optional	Alphanumeric	10	12345678
----------	----------	--------------	----	----------

#### Response.Token

The token that is assigned to the sent card information; responding to a "GenerateToken" flag with the value "Yes". This parameter is a part of the tokenization parameters, check the [Tokenization](#) section for more details.

Response	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27
----------	----------	--------------	----	--

#### Response.PaymentMethod

An Alphanumeric value to indicate which payment method will be used.

Supported values depend on the requested **version** as follows:

**If Version is 1.0 :**

- 1 → that means a payment using Card.
- 2 → that means a payment using SADAD.

**If Version is 2.0 :**

- 1:Card Name** (1 indicates Payment Method Card) e.g. **1:Visa**
- 2** (indicates Payment Method SADAD).

\* Possible Card Names are provided by SmartRoute operation team upon merchant enrollment.

Request	Conditional	Alphanumeric	42	2
---------	-------------	--------------	----	---

### 3.3. Direct Post Verify Message

This message is intended to perform a payment using the merchant's interface, then perform an automatic reversal after the payment is done, the main goal for this message is to verify the user's card information.

It's based on the Direct Post communication model as described in [Communication Model section](#).

#### 3.3.1. Request Fields: Basic Fields

Field Name				
Field Description				
Request/Response	Required/Optional	Field Type	Length	Sample Data

MessageID				
Alphanumeric value representing the action to be called, <b>12</b> for Direct Post Payment				
Request	Required	Alphanumeric	2	12

TransactionID				
The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				
Request	Required	Alphanumeric	20	1440954863817

MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Request	Required	Alphanumeric	40	MID0001

Amount				
A numeric value containing the Item purchase amount ISO Formatted with no decimal point.  e.g. 100 for 1.00 USD				
Request	Required	Numeric	9	100

CurrencyISOCode				
The numeric ISO Code for the currency and not the character value.  e.g. 840 for US Dollar 400 for JOD 682 for SAR 784 for AED				
Request	Required	Numeric	3	840

<b>PaymentMethod</b>				
A numeric value to indicate which payment method will be used. Supported values are: <b>1 →</b> which means a payment using Card. <b>2 →</b> which means a payment using SADAD.				
Request	Required	Numeric	1	2
<b>CardNumber</b>				
The customer's card number that will be used in the payment. This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
<b>Note: Shouldn't be included in the Secure Hash</b>				
Request	Conditional	Numeric	19	4111111111111111

<b>ExpiryDateYear</b>				
The customer's card expiry date year digits that will be used in the payment. The format of this parameter should be in the form (YY). This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
<b>Note: Shouldn't be included in the Secure Hash</b>				
Request	Conditional	Numeric	2	17

<b>ExpiryDateMonth</b>				
The customer's card expiry date month digits that will be used in the payment. The format of this parameter should be in the form (MM). This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
<b>Note: Shouldn't be included in the Secure Hash</b>				
Request	Conditional	Numeric	2	02

<b>SecurityCode</b>				
The customer's card Security Code (e.g. CVV or CVC) depending on the Card Type that will be used in the payment. This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
<b>Note: Shouldn't be included in the Secure Hash</b>				
Request	Conditional	Numeric	4	123

<b>CardHolderName</b>				
The customer's card holder name that will be used in the payment. This parameter is optional if the sent <b>PaymentMethod</b> parameter is 1 (Card). The format should be alphabetic with spaces allowed.				
<b>Note: Shouldn't be included in the Secure Hash</b>				

Request	Optional	Alphabetic	64	Card Holder Name
---------	----------	------------	----	------------------

#### PaymentDescription

Alphanumeric string containing a narrative description of the payment order using the language specified in the language parameter.

Request	Required	Alphanumeric	100	SamplePayment
---------	----------	--------------	-----	---------------

#### SadadOlpId

The customer's SADAD OLP ID that will be used in the payment. This parameter is required if the sent **PaymentMethod** parameter is 2 (SADAD).

**Note: Shouldn't be included in the Secure Hash**

Request	Conditional	Alphanumeric	12	Test123
---------	-------------	--------------	----	---------

#### SecureHash

Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string starting with the merchant's Merchant Authentication Token, then all parameters(required parameters and optional parameters if they are provided) except (**CardNumber, SecurityCode, CardHolderName, ExpiryDateYear, ExpiryDateMonth, SadadOlpId** since those parameters are entered by the customer (card holder) on the screen, and will be submitted directly to SmartRoute's URL, so they can't be captured and entered in the secure hash parameters.)

Ordered alphabetically by parameter's name should be part of the secure hash, with no separators and no terminating character.

Please refer to [Appendix B: Secure Hash – Direct Post Payment](#) for more details about secure hash generation

Request	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e
---------	----------	--------------	----	--

### 3.3.2. Response Fields: Basic Fields

#### Response.StatusCode

Alphanumeric value representing the response code, this code covers errors generated by SmartRoute.

Check [Appendix A: Direct Post Payment Response Codes](#) for descriptive details about Response Codes.

Response	Required	Alphanumeric	5	00000
----------	----------	--------------	---	-------

#### Response.StatusDescription

Alphanumeric value representing a message describing the response status as received from SmartRoute using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.

Response	Required	Alphanumeric	100	Payment processed successfully
----------	----------	--------------	-----	--------------------------------

Response.Amount				
A numeric value containing the total transaction amount ISO Formatted with no decimal point.				
e.g. 1.00 USD received as 100 1.00 SAR received as 100 1.00 AED received as 100 1.000 JOD received as 1000				
Response	Required	Numeric	9	100

Response.CurrencyISOCode				
The numeric ISO Code for the currency and not the character value.				
e.g. 840 for US Dollar 400 for JOD 682 for SAR 784 for AED				
Response	Required	Numeric	3	840

Response.MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Response	Required	Alphanumeric	40	MID0001

Response.TransactionID				
The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				
Response	Required	Alphanumeric	20	201508180000001

Response.MessageID				
Alphanumeric value representing the action to be called, <b>12</b> for Sale				
Response	Required	Alphanumeric	2	12

Response.SecureHash				
Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all response parameter appended in alphabetical				

order based on parameter's name, with no separators and no terminating character. Please refer to <a href="#">Appendix B: Secure Hash – Direct Post (Sale)</a> for more details about secure hash generation.				
Response	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e

### 3.3.3. Other Optional Fields

<b>Language</b>				
Alphabetic value representing the language of the interface displayed to customer at merchant site, and used as language for the payment description parameter. PG will use this value to display the interface supporting selected language to the customer during the payment process. Supported values are: En Ar				
Request	Optional	Alphanumeric	2	En

<b>ItemID</b>				
The custom item ID for the merchant.				
Request	Optional	Alphanumeric	25	Item1

<b>Version</b>				
A numeric value with (.) separator representing the version of the command to be used. Send it as 1.0. Send it as 2.0 to add Response.PaymentMethod to response.				
Request	Optional	Numeric	5	1.0

<b>Channel</b>				
The Channel to be used by SmartRoute System. It could be one of: 0 → E-Commerce, 1 → IVR 2 → POS				
Request	Optional	Numeric	1	0

<b>Quantity</b>				
A numeric value greater than ZERO represents the quantity of purchased Item				
Request	Optional	Numeric	5	1

<b>ResponseBackURL</b>				
Merchant site response page URL that will receive the response from SmartRoute, this can help merchant having different response pages based on the requested service or any other criteria				
Request	Optional	Alphanumeric	512	https://MerchantReplyURL/PaymentReply.do

<b>GenerateToken</b>				
----------------------	--	--	--	--

This flag indicates whether to generate a token for the sent card information or not. It accepts the values “Yes” and “No”. Sending this field as “No” acts like when the field is not sent at all. This parameter is a part of the tokenization parameters, check the <a href="#">Tokenization</a> section for more details.				
Request	Optional	Alphabetic	3	Yes

<b>Token</b>				
The token that will be used in this request; to represent a previously used card information. This parameter is a part of the tokenization parameters, check the <a href="#">Tokenization</a> section for more details.				
Request	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27

<b>Response.CardExpiryDate</b>				
Expiry date of the card (MMYY).				
Response	Optional	Alphanumeric	4	0416

<b>Response.CardHolderName</b>				
Card Holder Name				
Response	Optional	Alphanumeric	32	FName LName

<b>Response.CardNumber</b>				
Masked Card Number				
Response	Optional	Alphanumeric	19	4747*****123

<b>Response.GatewayStatusCode</b>				
Alphanumeric value representing the gateway response code, this code covers errors generated by the chosen gateway.				
Response	Optional	Alphanumeric	15	0000

<b>Response.GatewayStatusDescription</b>				
Alphanumeric value representing a message describing the response status as received from the chosen gateway using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Response	Optional	Alphanumeric	100	Sample Gateway Description

<b>Response.GatewayName</b>				
This value represents the gateway name that processed the transaction, it can be alphanumeric with some special characters like space, '@' and '_ '.				
Response	Optional	Alphanumeric and Some Special	40	TestGateway

<b>Response.RRN</b>				
---------------------	--	--	--	--

Alphanumeric value representing a Receipt Reference Number as a reference for the current payment transaction. This value will be returned if the value is provided from the gateway.

Response	Optional	Alphanumeric	60	201508201600462840000000000
----------	----------	--------------	----	-----------------------------

#### Response.ApprovalCode

Approval Code received from Payment Processor such as Visa. It will be return only when the transaction is success. This value will be returned if the value is provided from the gateway.

Response	Optional	Alphanumeric	10	12345678
----------	----------	--------------	----	----------

#### Response.Token

The token that is assigned to the sent card information; responding to a "GenerateToken" flag with the value "Yes". This parameter is a part of the tokenization parameters, check the [Tokenization](#) section for more details.

Response	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbc85aed1b4173ed604f8fd5fa3cf72a02e27
----------	----------	--------------	----	---

#### Response.PaymentMethod

An Alphanumeric value to indicate which payment method will be used.

Supported values depend on the requested **version** as follows:

**If Version is 1.0 :**

- 1 → that means a payment using Card.
- 2 → that means a payment using SADAD.

**If Version is 2.0 :**

- 1: **Card Name** (1 indicates Payment Method Card) e.g. 1: **Visa**
- 2 (indicates Payment Method SADAD).

\* Possible Card Names are provided by SmartRoute operation team upon merchant enrollment.

Request	Conditional	Alphanumeric	42	2
---------	-------------	--------------	----	---

### 3.4. API Payment – API Pre-Authorization

This message is intended to perform a payment. It's based on the API communication model as described in [Communication Model](#) section.

After performing an API Payment or an API Pre-Authorization, and if the 'Response.StatusCode' parameter was (20001 or 20002), the merchant should handle the authentication process for credit cards and SADAD payments. Then an API Approve message must follow to pass any authentication data to the payment gateway. Otherwise, there will be no need for an API Approve following an API Payment. You can refer to the appendix for further details about credit card and SADAD authentication process.

There are two types of messages that can be used:

- API Payment
- API Pre-Authorization

### 3.4.1. Request Fields: Basic Fields

Field Name				
Field Description				
Request/Response	Required/Optional	Field Type	Length	Sample Data

MessageID				
Alphanumeric value representing the action to be called:				
<ul style="list-style-type: none"> <li>• <b>8</b> For API Payment</li> <li>• <b>13</b> For API Pre-Authorization</li> </ul>				
Request	Required	Alphanumeric	2	1

TransactionID				
The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				
Request	Required	Alphanumeric	20	1440954863817

MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Request	Required	Alphanumeric	40	MID0001

Amount				
A numeric value containing the Item purchase amount ISO Formatted with no decimal point. e.g. 100 for 1.00 USD				
Request	Required	Numeric	9	100

CurrencyISOCode				
The numeric ISO Code for the currency and not the character value.  e.g. 840 for US Dollar 400 for JOD 682 for SAR 784 for AED				
Request	Required	Numeric	3	840
PaymentMethod				
A numeric value to indicate which payment method will be used. Supported values are:				

1 → which means a payment using Card.				
2 → which means a payment using SADAD.				
Request	Required	Numeric	1	2

<b>CardNumber</b>				
The customer's card number that will be used in the payment. This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
Request	Conditional	Numeric	19	4111111111111111

<b>ExpiryDateYear</b>				
The customer's card expiry date year digits that will be used in the payment. The format of this parameter should be in the form (YY). This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
Request	Conditional	Numeric	2	17

<b>ExpiryDateMonth</b>				
The customer's card expiry date month digits that will be used in the payment. The format of this parameter should be in the form (MM). This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
Request	Conditional	Numeric	2	02

<b>SecurityCode</b>				
The customer's card Security Code (e.g. CVV or CVC) depending on the Card Type that will be used in the payment. This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
Request	Conditional	Numeric	4	123

<b>SadadOlpId</b>				
The customer's SADAD OLP ID that will be used in the payment.				
This parameter is required if the sent <b>PaymentMethod</b> parameter is 2 (SADAD).				
Request	Conditional	Alphanumeric	12	Test123

<b>mfu</b>				
This parameter represents the Merchant Forward URL which SADAD will use to redirect the customer back to the Merchant and is used as a parameter when redirecting the customer to SADAD.				
Please refer to <a href="#">Appendix E: SADAD Implementation</a> for more details about Redirecting to SASDAD				

This parameter is required if the sent <b>PaymentMethod</b> parameter is 2 ( <i>SADAD</i> ) and the Transaction requires authentication.				
Request	Conditional	Alphanumeric	N/A	<a href="https://MerchantSite.com/SadadResponse.do">https://MerchantSite.com/SadadResponse.do</a>

<b>ClientIPaddress</b>				
A value representing the client's <u>public</u> IP Address				
Request	Required	Alphanumeric	19	79.183.118.666

<b>PaymentDescription</b>				
Alphanumeric string containing a narrative description of the payment order using the language specified in the language parameter. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Request	Required	Alphanumeric	100	SamplePayment

<b>SecureHash</b>				
Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all parameters (required parameters and optional parameters if they are provided) Ordered alphabetically by parameter's name should be part of the secure hash, with no separators and no terminating character. Please refer to <a href="#">Appendix B: Secure Hash – API Payment</a> for more details about secure hash generation				
Request	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e

### 3.4.2. Response Fields: Basic Fields

<b>Response.StatusCode</b>				
Alphanumeric value representing the response code, this code covers errors generated by SmartRoute. Check <a href="#">Appendix A: API Payment Response Codes</a> for descriptive details about Response Codes.				
Response	Required	Alphanumeric	5	00000

<b>Response.StatusDescription</b>				
Alphanumeric value representing a message describing the response status as received from SmartRoute using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Response	Required	Alphanumeric	100	Payment processed successfully

Response.Amount				
A numeric value containing the total transaction amount ISO Formatted with no decimal point.				
e.g. 1.00 USD received as 100 1.00 SAR received as 100 1.00 AED received as 100 1.000 JOD received as 1000				

Response	Required	Numeric	9	100
Response.CurrencyISOCode				
The numeric ISO Code for the currency and not the character value.				
e.g. 840 for US Dollar 400 for JOD 682 for SAR 784 for AED				
Response	Required	Numeric	3	840

Response.MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Response	Required	Alphanumeric	40	MID0001

Response.TransactionID				
The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				
Response	Required	Alphanumeric	20	201508180000001

Response.MessageID				
Alphanumeric value representing the called action:				
<ul style="list-style-type: none"> <li>• <b>8</b> for <b>API Payment</b></li> <li>• <b>13</b> for <b>API Pre-Authorization</b></li> </ul>				
Response	Required	Alphanumeric	2	1

Response.SecureHash				
Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all response parameter appended in alphabetical order based on parameter's name, with no separators and no terminating character. Please refer to <a href="#">Appendix B: Secure Hash – API Payment</a> for more details about secure hash generation.				
Response	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5

				d7bf7da30f4f2e62b89df74a2e
--	--	--	--	----------------------------

Response.PaymentMethod				
<p>An Alphanumeric value to indicate which payment method will be used. Supported values depend on the requested <b>version</b> as follows:</p> <p><b>If Version is 1.0 :</b></p> <p>1 → that means a payment using Card. 2 → that means a payment using SADAD.</p> <p><b>If Version is 2.0 :</b></p> <p>1:Card Name (1 indicates Payment Method Card) e.g. 1:Visa 2 (indicates Payment Method SADAD).</p> <p>* Possible Card Names are provided by SmartRoute operation team upon merchant enrollment.</p>				
Request	Required	Alphanumeric	42	2

Response.estn				
<p>This parameter represents Encrypted SADAD Transaction Number and is used as a parameter when redirecting the customer to SADAD. Please refer to <a href="#">Appendix E: SADAD Implementation</a> for more details about Redirecting to SADAD. This parameter is required if the sent <b>PaymentMethod</b> parameter is 2 (SADAD) and the Transaction requires authentication.</p>				
Response	Conditional	Alphanumeric	N/A	Q1NIYzArNTdEd3ZSVjQ0S0JxN0ppMW5 ObjFIUmVsdEtOMzRpaDBicWFPSGJMVjJ MaHpBdzloaDB1SWlrWkxFck0xNHVaL3F yWnNzVFVianBTWjdlQmtDek1UbHBodU RpdINGNXBicWxHaHY2Q0E0cVVWMXJQ YINpNVBmN2I3ZXIESWpuVTF6dGRDcU9I QWw1eHpQK2RCSWs3aFhueHVIb2JUa=

Response.mfu				
<p>This parameter represents the Merchant Forward URL which SADAD will use to redirect back the customer back to the Merchant and is used as a parameter when redirecting the customer to SADAD. Please refer to <a href="#">Appendix E: SADAD Implementation</a> for more details about Redirecting to SADAD</p> <p>This parameter is required if the sent <b>PaymentMethod</b> parameter is 2 (SADAD) and the Transaction requires authentication.</p>				
Response	Conditional	Alphanumeric	N/A	<a href="https://MerchantSite.com/SadadResponse.do">https://MerchantSite.com/SadadResponse.do</a>

Response.PaReq				
Payment Authentication Request Used for 3DS payment.				

Please refer to [Appendix D: 3D-Secure Implementation](#) for more details about Redirecting to 3D-Secure

This parameter is required if the sent **PaymentMethod** parameter is 1 (*Card*) and the Transaction requires authentication (API Approve)

Response	Conditional	Alphanumeric	N/A	eJxVUttu4jAQ/ZWqH4AvJCxBgyVikJo
----------	-------------	--------------	-----	---------------------------------

### 3.4.3. Other Optional Fields

CardHolderName				
The customer's card holder name that will be used in the payment. This parameter is optional if the sent <b>PaymentMethod</b> parameter is 1 (Card). The format should be alphabetic with spaces allowed.				
Request	Optional	Alphabetic	64	Card Holder Name

ItemID				
The custom item ID for the merchant.				
Request	Optional	Alphanumeric	25	Item1

Channel				
The Channel to be used by SmartRoute System. It could be one of: 0 → E-Commerce, 1 → IVR 2 → POS				
Request	Optional	Numeric	1	0

Quantity				
A numeric value greater than ZERO represents the quantity of purchased Item				
Request	Optional	Numeric	5	1

Version				
A numeric value with (.) separator representing the version of the command to be used. Send it as 1.0. Send it as 2.0 to: 1- Add Response.PaymentMethod to Response Fields. 2- Use the RecurringSeriesID field.				
Request	Optional	Numeric	5	1.0

FrameworkInfo				
An alphanumeric value representing the client's used framework.				
Request	Optional	Alphanumeric	30	Android 7.0

GenerateToken				
---------------	--	--	--	--

This flag indicates whether to generate a token for the sent card information or not. It accepts the values “Yes” and “No”. Sending this field as “No” acts like when the field is not sent at all. This parameter is a part of the tokenization parameters, check the <a href="#">Tokenization</a> section for more details.				
Request	Optional	Alphabetic	3	Yes

<b>Token</b>				
The token that will be used in this request; to represent a previously used card information. This parameter is a part of the tokenization parameters, check the <a href="#">Tokenization</a> section for more details.				
Request	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27

<b>RecurringSeriesID</b>				
The series id that will be used in this request; to represent the card number that will be used in this transaction. The same value should be provided when performing a recurring payment.				
This field is supported only if the Version field is set to 2.0				
Request	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27

<b>Response.GatewayStatusCode</b>				
Alphanumeric value representing the gateway response code, this code covers errors generated by the chosen gateway.				
Response	Optional	Alphanumeric	15	0000

<b>Response.GatewayStatusDescription</b>				
Alphanumeric value representing a message describing the response status as received from the chosen gateway using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Response	Optional	Alphanumeric	100	Sample Gateway Description

<b>Response.GatewayName</b>				
This value represents the gateway name that processed the transaction, it can be alphanumeric with some special characters like space, '@' and '_'.				
Response	Optional	Alphanumeric and Some Special	40	TestGateway

<b>Response.RRN</b>				
Alphanumeric value representing a Receipt Reference Number as a reference for the current payment transaction. This value will be returned if the value is provided from the gateway.				
Response	Optional	Alphanumeric	60	2015082016004628400000000000

<b>Response.ApprovalCode</b>				
------------------------------	--	--	--	--

Approval Code received from Payment Processor such as Visa. It will be returned only when the transaction is success. This value will be returned if the value is provided from the gateway.				
Response	Optional	Alphanumeric	10	12345678

<b>Response.AuthenticationURL</b>				
The Authentication URL represents the either SADAD URL or 3D-Secure URL which the Merchant will use to redirect the customer to in order to authenticate the payment.				
Response	Optional	Alphanumeric	N/A	https://anb.com.sa/anb-micro/spring/login

<b>Response.Token</b>				
The token that is assigned to the sent card information; responding to a "GenerateToken" flag with the value "Yes". This parameter is a part of the tokenization parameters, check the <a href="#">Tokenization</a> section for more details.				
Response	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27

### 3.5. API mPayment

This message is intended to perform a payment. It's based on the API communication model as described in [Communication Model section](#).

After performing an API **mPayment**, and if the 'Response.StatusCode' parameter was (20002), the merchant should handle the authentication process for SADAD payments. Then an API Approve message must follow to pass any authentication data to the payment gateway. Otherwise, there will be no need for an API Approve following an API **mPayment**. You can refer to the appendix for further details about SADAD authentication process.

#### 3.5.1. Request Fields: Basic Fields

<b>Field Name</b>				
<b>Field Description</b>				
<b>Request/Response</b>	<b>Required/Optional</b>	<b>Field Type</b>	<b>Length</b>	<b>Sample Data</b>

<b>MessageID</b>				
Alphanumeric value representing the action to be called, <b>9</b> for API <i>mPayment</i>				
Request	Required	Alphanumeric	2	1

<b>TransactionID</b>				
The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				
Request	Required	Alphanumeric	20	1440954863817

MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Request	Required	Alphanumeric	40	MID0001

Amount				
A numeric value containing the Item purchase amount ISO Formatted with no decimal point. e.g. 100 for 1.00 USD				
Request	Required	Numeric	9	100

CurrencyISOCode				
The numeric ISO Code for the currency and not the character value.  e.g. 840 for US Dollar 400 for JOD 682 for SAR 784 for AED				
Request	Required	Numeric	3	840

PaymentMethod				
A numeric value to indicate which payment method will be used. Supported values are: <b>1 →</b> which means a payment using Card. <b>2 →</b> which means a payment using SADAD.				
Request	Required	Numeric	1	2

CardNumber				
The customer's card number that will be used in the payment. This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
Request	Conditional	Numeric	19	4111111111111111

ExpiryDateYear				
The customer's card expiry date year digits that will be used in the payment. The format of this parameter should be in the form (YY). This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
Request	Conditional	Numeric	2	17

ExpiryDateMonth				
The customer's card expiry date month digits that will be used in the payment. The format of this parameter should be in the form (MM). This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
Request	Conditional	Numeric	2	02

SecurityCode				
The customer's card Security Code (e.g. CVV or CVC) depending on the Card Type that will be used in the payment. This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
Request	Conditional	Numeric	4	123

SadadOlpId				
The customer's SADAD OLP ID that will be used in the payment. This parameter is required if the sent <b>PaymentMethod</b> parameter is 2 (SADAD).				
Request	Conditional	Alphanumeric	12	Test123

mfu				
<p>This parameter represents the Merchant Forward URL which SADAD will use to redirect back the customer back to the Merchant and is used as a parameter when redirecting the customer to SADAD.</p> <p>Please refer to <a href="#">Appendix E: SADAD Implementation</a> for more details about Redirecting to SADAD</p> <p>This parameter is required if the sent <b>PaymentMethod</b> parameter is 2 (SADAD) and the Transaction requires authentication.</p>				
Request	Conditional	Alphanumeric	N/A	<a href="https://MerchantSite.com/SadadResponse.do">https://MerchantSite.com/SadadResponse.do</a>

ClientIPaddress				
A value representing the client's <u>public</u> IP Address				
Request	Required	Alphanumeric	19	79.183.118.122

PaymentDescription				
<p>Alphanumeric string containing a narrative description of the payment order using the language specified in the language parameter.</p> <p>This value should be UTF-8 encoded when it is entered into the secure hash generation process.</p>				
Request	Required	Alphanumeric	1000	SamplePayment

SecureHash				
<p>Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all parameters(required parameters and optional parameters if they are provided) Ordered alphabetically by parameter's name should be part of the secure hash, with no separators and no terminating character.</p> <p>Please refer to <a href="#">Appendix B: Secure Hash – API mPayment</a> for more details about secure hash generation</p>				
Request	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e

### 3.5.2. Response Fields: Basic Fields

#### Response.StatusCode

Alphanumeric value representing the response code, this code covers errors generated by SmartRoute.

Check [Appendix A: API mPayment Response Codes](#) for descriptive details about Response Codes.

Response	Required	Alphanumeric	5	00000
----------	----------	--------------	---	-------

#### Response.StatusDescription

Alphanumeric value representing a message describing the response status as received from SmartRoute using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.

Response	Required	Alphanumeric	100	Payment processed successfully
----------	----------	--------------	-----	--------------------------------

#### Response.Amount

A numeric value containing the total transaction amount ISO Formatted with no decimal point.

e.g.

1.00 USD received as 100

1.00 SAR received as 100

1.00 AED received as 100

1.000 JOD received as 1000

Response	Required	Numeric	9	100
----------	----------	---------	---	-----

#### Response.CurrencyISOCode

The numeric ISO Code for the currency and not the character value.

e.g.

840 for US Dollar

400 for JOD

682 for SAR

784 for AED

Response	Required	Numeric	3	840
----------	----------	---------	---	-----

#### Response.MerchantID

Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.

Response	Required	Alphanumeric	40	MID0001
----------	----------	--------------	----	---------

#### Response.TransactionID

The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.

Response	Required	Alphanumeric	20	2015081800000001
----------	----------	--------------	----	------------------

Response.MessageID				
Alphanumeric value representing the action to be called, <b>9</b> for <b>API mPayment</b>				
Response	Required	Alphanumeric	2	1

Response.SecureHash				
Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all response parameter appended in alphabetical order based on parameter's name, with no separators and no terminating character. Please refer to <u>Appendix B: Secure Hash – API mPayment</u> for more details about secure hash generation.				
Response	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e

Response.PaymentMethod				
An Alphanumeric value to indicate which payment method will be used. Supported values depend on the requested <b>version</b> as follows: <b>If Version is 1.0 :</b> <b>1 →</b> that means a payment using Card. <b>2 →</b> that means a payment using SADAD.  <b>If Version is 2.0 :</b> <b>1:Card Name</b> (1 indicates Payment Method Card) e.g. <b>1:Visa</b> <b>2</b> (indicates Payment Method SADAD).  * Possible Card Names are provided by SmartRoute operation team upon merchant enrollment.				
Request	Required	Alphanumeric	42	2

Response.estn				
This parameter represents Encrypted SADAD Transaction Number and is used as a parameter when redirecting the customer to SADAD. Please refer to <u>Appendix E: SADAD Implementation</u> for more details about Redirecting to SADAD  This parameter is required if the sent <b>PaymentMethod</b> parameter is 2 ( <b>SADAD</b> ) and the Transaction requires authentication.				
Response	Conditional	Alphanumeric	N/A	Q1NIYzArNTdEd3ZSVjQ0S0JxN0ppMW5ObjFIUmVsdEtOMzRpaDBicWFPSGJMVJlMaHpBdzloaDB1SWlrWkxFck0xNHVaL3FyWnNzVfVianBTWjdIQmtDek1UbHBodURpdINGNXBicWxHaHY2Q0E0cVVWMXJQYINpNVBmN2l3ZXIESWpuVTF6dGRDcU9lQWw1eHpQK2RCSWs3aFhueHvIb2JUa=

Response.mfu				
<p>This parameter represents the Merchant Forward URL which SADAD will use to redirect back the customer back to the Merchant and is used as a parameter when redirecting the customer to SADAD.</p> <p>Please refer to <a href="#">Appendix E: SADAD Implementation</a> for more details about Redirecting to SADAD</p> <p>This parameter is required if the sent <b>PaymentMethod</b> parameter is 2 (SADAD) and the Transaction requires authentication.</p>				
Response	Conditional	Alphanumeric	N/A	<a href="https://MerchantSite.com/SadadResponse.do">https://MerchantSite.com/SadadResponse.do</a>

### 3.5.3. Other Optional Fields

CardHolderName				
<p>The customer's card holder name that will be used in the payment. This parameter is optional if the sent <b>PaymentMethod</b> parameter is 1 (Card). The format should be alphabetic with spaces allowed.</p>				
Request	Optional	Alphabetic	64	Card Holder Name

ItemID				
<p>The custom item ID for the merchant.</p>				
Request	Optional	Alphanumeric	25	Item1

Channel				
<p>The Channel to be used by SmartRoute System. It could be one of:</p> <p>0 → E-Commerce, 1 → IVR 2 → POS</p>				
Request	Optional	Numeric	1	0

Quantity				
<p>A numeric value greater than ZERO represents the quantity of purchased Item</p>				
Request	Optional	Numeric	5	1

Version				
<p>A numeric value with (.) separator representing the version of the command to be used.</p> <p>Send it as 1.0.</p> <p>Send it as 2.0 to change Response.PaymentMethod format.</p>				
Request	Optional	Numeric	5	1.0

FrameworkInfo				
<p>An alphanumeric value representing the client's used framework.</p>				
Request	Optional	Alphanumeric	30	Android 7.0

GenerateToken				
This flag indicates whether to generate a token for the sent card information or not. It accepts the values “Yes” and “No”. Sending this field as “No” acts like when the field is not sent at all. This parameter is a part of the tokenization parameters, check the <a href="#">Tokenization</a> section for more details.				
Request	Optional	Alphabetic	3	Yes

Token				
The token that will be used in this request; to represent a previously used card information. This parameter is a part of the tokenization parameters, check the <a href="#">Tokenization</a> section for more details.				
Request	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27

Response.GatewayStatusCode				
Alphanumeric value representing the gateway response code, this code covers errors generated by the chosen gateway.				
Response	Optional	Alphanumeric	15	0000

Response.GatewayStatusDescription				
Alphanumeric value representing a message describing the response status as received from the chosen gateway using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Response	Optional	Alphanumeric	100	Sample Gateway Description

Response.GatewayName				
This value represents the gateway name that processed the transaction, it can be alphanumeric with some special characters like space, '@' and '_'.				
Response	Optional	Alphanumeric and Some Special	40	TestGateway

Response.RRN				
Alphanumeric value representing a Receipt Reference Number as a reference for the current payment transaction. This value will be returned if the value is provided from the gateway.				
Response	Optional	Alphanumeric	60	2015082016004628400000000000

Response.ApprovalCode				
Approval Code received from Payment Processor such as Visa. It will be returned only when the transaction is success. This value will be returned if the value is provided from the gateway.				
Response	Optional	Alphanumeric	10	12345678

Response.AuthenticationURL				
----------------------------	--	--	--	--

<p>The Authentication URL, in case of an <b>API mPayment</b>, represents the SADAD URL which the Merchant will use to redirect the customer to in order to complete the payment. Please refer to <a href="#">Appendix E: SADAD Implementation</a> for more details about Redirecting to SADAD.</p> <p>This parameter is required if the sent <b>PaymentMethod</b> parameter is 2 (<i>SADAD</i>) and the Transaction requires authentication.</p>				
Response	Optional	Alphanumeric	N/A	https://anb.com.sa/anb-micro/spring/login

<b>Response.Token</b>				
The token that is assigned to the sent card information; responding to a “GenerateToken” flag with the value “Yes”. This parameter is a part of the tokenization parameters, check the <a href="#">Tokenization</a> section for more details.				
Response	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27

## 3.6. API Approve

This message is intended to approve an API Payment or an API mPayment if needed. It's based on the API communication model as described in [Communication Model](#) section.

### 3.6.1. Request Fields: Basic Fields

<b>Field Name</b>				
<b>Field Description</b>				
<b>Request/Response</b>	<b>Required/Optional</b>	<b>Field Type</b>	<b>Length</b>	<b>Sample Data</b>

<b>MessageID</b>				
Alphanumeric value representing the action to be called, <b>10</b> for Approve Payment				
Request	Required	Alphanumeric	2	1

<b>TransactionID</b>				
The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction. In this case (API Approve), the TransactionID, shall be the same one used for the API Payment or API mPayment.				
Request	Required	Alphanumeric	20	1440954863817

<b>MerchantID</b>				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Request	Required	Alphanumeric	40	MID0001

<b>PaymentMethod</b>				
A numeric value to indicate which payment method will be used. Supported values are:				

1 → which means a payment using Card.				
2 → which means a payment using SADAD.				
Request	Required	Numeric	1	2

<b>estn</b>				
This field represents <b>Encrypted SADAD Transaction Number</b> which is returned to the merchant from SADAD.				
This parameter is required if the <b>PaymentMethod</b> is 2 (SADAD)				
Request	Conditional	Alphanumeric	12	Test123

<b>PARes</b>				
Payment Authentication Response. Used in 3DS payment process.				
This parameter is required if the <b>PaymentMethod</b> is 1 (Card) and when approving an API Payment.				
Request	Conditional	Alphanumeric	N/A	eJzFV2mTokoW/Ssd9T4a3ewiHZQvkh2 ...

<b>CardNumber</b>				
The customer's card number that will be used in the payment. This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
Request	Conditional	Numeric	19	4111111111111111

<b>ExpiryDateYear</b>				
The customer's card expiry date year digits that will be used in the payment. The format of this parameter should be in the form (YY). This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
Request	Conditional	Numeric	2	17

<b>ExpiryDateMonth</b>				
The customer's card expiry date month digits that will be used in the payment. The format of this parameter should be in the form (MM). This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
Request	Conditional	Numeric	2	02

<b>SecurityCode</b>				
The customer's card Security Code (e.g. CVV or CVC) depending on the Card Type that will be used in the payment. This parameter is required if the sent <b>PaymentMethod</b> parameter is 1 (Card).				
Request	Conditional	Numeric	4	123

SecureHash				
<p>Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all parameters(required parameters and optional parameters if they are provided)</p> <p>Ordered alphabetically by parameter's name should be part of the secure hash, with no separators and no terminating character.</p> <p>Please refer to <a href="#">Appendix B: Secure Hash – API Approve</a> for more details about secure hash generation</p>				
Request	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbe a27bc5d7bf7da30f4f2e62b89df74a24

### 3.6.2. Response Fields: Basic Fields

Response.StatusCode				
<p>Alphanumeric value representing the response code, this code covers errors generated by SmartRoute.</p> <p>Check <a href="#">Appendix A: API Approve Response Codes</a> for descriptive details about Response Codes.</p>				
Response	Required	Alphanumeric	5	00000

Response.StatusDescription				
<p>Alphanumeric value representing a message describing the response status as received from SmartRoute using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.</p>				
Response	Required	Alphanumeric	100	Payment processed successfully

Response.Amount				
<p>A numeric value containing the total transaction amount ISO Formatted with no decimal point.</p> <p>e.g.  1.00 USD received as 100  1.00 SAR received as 100  1.00 AED received as 100  1.000 JOD received as 1000</p>				
Response	Required	Numeric	9	100

Response.CurrencyISOCode				
<p>The numeric ISO Code for the currency and not the character value.</p> <p>e.g.  840 for US Dollar  400 for JOD</p>				

682 for SAR 784 for AED				
Response	Required	Numeric	3	840

#### Response.MerchantID

Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.

Response	Required	Alphanumeric	40	MID0001
----------	----------	--------------	----	---------

#### Response.TransactionID

The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.

Response	Required	Alphanumeric	20	201508180000001
----------	----------	--------------	----	-----------------

#### Response.MessageID

Alphanumeric value representing the action to be called, **10 for API Approve**

Response	Required	Alphanumeric	2	1
----------	----------	--------------	---	---

#### Response.SecureHash

Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string starting with the merchant's Merchant Authentication Token, then all response parameter appended in alphabetical order based on parameter's name, with no separators and no terminating character. Please refer [Appendix B: Secure Hash – API Approve](#) for more details about secure hash generation.

Response	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbb ea27bc5d7bf7da30f4f2e62b89df74a 2e
----------	----------	--------------	----	--

### 3.6.3. Other Optional Fields

#### CardHolderName

The customer's card holder name that will be used in the payment. This parameter is optional if the sent **PaymentMethod** parameter is 1 (Card). The format should be alphabetic with spaces allowed.

Request	Optional	Alphabetic	64	Card Holder Name
---------	----------	------------	----	------------------

#### Response.GatewayStatusCode

Alphanumeric value representing the gateway response code, this code covers errors generated by the chosen gateway.

Response	Optional	Alphanumeric	15	0000
----------	----------	--------------	----	------

#### Response.GatewayStatusDescription

Alphanumeric value representing a message describing the response status as received from the chosen gateway using the language specified in the request; this parameter will

be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Response	Optional	Alphanumeric	100	Sample Gateway Description

<b>Response.GatewayName</b>				
This value represents the gateway name that processed the transaction, it can be alphanumeric with some special characters like space, '@' and '_'.				
Response	Optional	Alphanumeric and Some Special	40	TestGateway

<b>Response.RRN</b>				
Alphanumeric value representing a Receipt Reference Number as a reference for the current payment transaction. This value will be returned if the value is provided from the gateway.				
Response	Optional	Alphanumeric	60	2015082016004628400000000000

<b>Response.ApprovalCode</b>				
Approval Code received from Payment Processor such as Visa. It will be return only when the transaction is success. This value will be returned if the value is provided from the gateway.				
Response	Optional	Alphanumeric	10	12345678

<b>Response.Token</b>				
The token that is assigned to the sent card information; responding to a "GenerateToken" flag with the value "Yes". This parameter is a part of the tokenization parameters, check the <a href="#">Tokenization</a> section for more details.				
Response	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27

### 3.7. Inquiry Message

This message is intended to perform a Transaction status Inquiry It's based on the Back-To-Back communication model as described in [Communication Model](#) section.

#### 3.7.1. Request Fields

<b>Field Name</b>				
<b>Field Description</b>				
<b>Request/Response</b>	<b>Required/Optional</b>	<b>Field Type</b>	<b>Length</b>	<b>Sample Data</b>

<b>MessageID</b>				
Alphanumeric value representing the action to be called, <b>2</b> for Inquiry Status Transaction				
Request	Required	Alphanumeric	2	2

<b>MerchantID</b>				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				

Request	Required	Alphanumeric	40	MID0001
---------	----------	--------------	----	---------

#### OriginalTransactionID

The transaction ID of the original transaction, which is needed to inquire about.

Request	Required	Alphanumeric	20	1440594083737
---------	----------	--------------	----	---------------

#### Version

A numeric value with (.) separator representing the version of the command to be used. Send it as 1.0

Request	Optional	Numeric	5	1.0
---------	----------	---------	---	-----

#### SecureHash

Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string starting with the merchant's Merchant Authentication Token, then all parameters(required parameters and optional parameters if they are provided) ordered alphabetically by parameter's name should be part of the secure hash, with no separators and no terminating character. Please refer to [Appendix B: Secure Hash – Transaction Inquiry](#) for more details about secure hash generation

Request	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318 edc283bbbea27bc5d7bf7d a30f4f2e62b89df74a2e
---------	----------	--------------	----	--

### 3.7.2. Response Fields

#### Response.MessageStatus

Alphanumeric value representing the response code, this code covers errors generated by SmartRoute. Check [Appendix A: Transaction Inquiry Response Codes](#) for descriptive details about Response Codes.

Response	Required	Alphanumeric	5	00000
----------	----------	--------------	---	-------

#### Response.StatusCode

Alphanumeric value representing the status of the Original transaction status – the transaction to be inquired about it.

Response	Required	Alphanumeric	5	00000
----------	----------	--------------	---	-------

#### Response.GatewayStatusCode

Alphanumeric value representing the gateway status of the Original transaction status – the transaction to be inquired about it.

Response	Optional	Alphanumeric	15	0000
----------	----------	--------------	----	------

#### Response.GatewayStatusDescription

Alphanumeric value representing a message describing the response status as received from the chosen gateway using the language specified in the request. This value is for the

original transaction – the transaction to be inquired about it. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Response	Optional	Alphanumeric	100	Sample Gateway Description

<b>Response.GatewayName</b>				
This value represents the gateway name that processed the transaction, it can be alphanumeric with some special characters like space, '@' and '_'.				
Response	Optional	Alphanumeric and Some Special	40	TestGateway

<b>Response.RRN</b>				
Alphanumeric value representing a Receipt Reference Number as a reference for the current payment transaction. This value will be returned if the value is provided from the gateway.				
Response	Optional	Alphanumeric	60	2015082016004628400000000000

<b>Response.ApprovalCode</b>				
Approval Code received from Payment Processor such as Visa. It will be return only when the transaction is success. This value will be returned if the value is provided from the gateway.				
Response	Optional	Alphanumeric	10	12345678

<b>Response.Amount</b>				
A numeric value containing the total transaction amount ISO Formatted with no decimal point.  e.g. 1.00 USD received as 100 1.00 SAR received as 100 1.00 AED received as 100 1.000 JOD received as 1000				
Response	Required	Numeric	9	100

<b>Response.CurrencyISOCode</b>				
The numeric ISO Code for the currency and not the character value.  e.g. 840 for US Dollar 400 for JOD 682 for SAR 784 for AED				
Response	Required	Numeric	3	840

<b>Response.MerchantID</b>				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Response	Required	Alphanumeric	40	MID0001
<b>Response.TransactionID</b>				

The transaction id of the original transaction, which is needed to inquiry about.				
Response	Required	Alphanumeric	20	201508180000001

<b>Response.MessageID</b>				
Alphanumeric value representing the action to be called, <b>2</b> for Inquiry Status Transaction				
Response	Required	Alphanumeric	2	2

<b>Response.CardExpiryDate</b>				
Expiry date of the card (MMYY).				
Response	Optional	Alphanumeric	4	1508

<b>Response.CardHolderName</b>				
Card Holder Name				
Response	Optional	Alphanumeric	32	FName LName

<b>Response.CardNumber</b>				
Masked Card Number				
Response	Optional	Alphanumeric	19	4747*****123

<b>Response.Token</b>				
If the Card details used in this transaction has token, it will be returned. This parameter is a part of the tokenization parameters, check the <a href="#">Tokenization</a> section for more details.				
Response	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27

<b>Response.ReversalStatus</b>				
The Reversal Status of the transaction to be inquired about it, possible values are: <b>0 → Reversal Required</b> <b>1 → Reversal Not Required</b> <b>2 → Reversal Successful</b> <b>3 → Reversal Failed</b>				
Response	Required	Numeric	1	1

<b>Response.PaymentMethod</b>				
A value to indicate which payment method was used. Supported values are: <b>1:Card Name</b> (1 indicates Payment Method Card) e.g. <b>1:Visa</b> <b>2</b> (indicates Payment Method SADAD).				
Request	Conditional	Alphanumeric	42	1 : Visa

<b>Response.SecureHash</b>				
Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all response parameter appended in alphabetical order based on parameter's name, with no separators and no terminating character.				

Please refer to <a href="#">Appendix B: Secure Hash – Transaction Inquiry</a> . For more details about secure hash generation.				
Response	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e

### 3.8. Refund Message

This message is intended to perform a transaction refund. It's based on the Back-To-Back communication model as described in [Communication Model](#) section.

#### 3.8.1. Request Fields

Field Name				
Field Description				
Request/Response	Required/Optional	Field Type	Length	Sample Data

MessageID				
Alphanumeric value representing the action to be called, <b>4</b> for the refund transaction.				
Request	Required	Alphanumeric	2	3

MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Request	Required	Alphanumeric	40	MID0001

TransactionID				
The transaction ID generated by the merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				
Request	Required	Alphanumeric	20	1440954863817

OriginalTransactionID				
The transaction ID of the original transaction, which is needed to refund it.				
Request	Required	Alphanumeric	20	1440594083737

Amount				
A numeric value containing the Item purchase amount ISO Formatted with no decimal point.  e.g. 100 for 1.00 USD				
Request	Required	Numeric	9	100

CurrencyISOCode				
The numeric ISO Code for the currency and not the character value.  e.g.				

840 for US Dollar 400 for JOD 682 for SAR 784 for AED				
Request	Required	Numeric	3	840

<b>Version</b>				
A numeric value with (.) separator representing the version of the command to be used. Send it as 1.0				
Request	Optional	Numeric	5	1.0

<b>SecureHash</b>				
Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all parameters(required parameters and optional parameters if they are provided) ordered alphabetically by parameter's name should be part of the secure hash, with no separators and no terminating character. Please refer to <a href="#">Appendix B: Secure Hash – Refund Transaction Action</a> for more details about secure hash generation				
Request	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318 edc283bbbea27bc5d7bf7d a30f4f2e62b89df74a2e

### 3.8.2. Response Fields

<b>Response.StatusCode</b>				
Alphanumeric value representing the response code, this code covers errors generated by SmartRoute. Check <a href="#">Appendix A: Refund Response Codes</a> for descriptive details about Response Codes.				
Response	Required	Alphanumeric	5	00000

<b>Response.OriginalTransactionID</b>				
The transaction ID of the original transaction, which is needed to void it.				
Request	Required	Alphanumeric	20	1440594083737

<b>Response.TransactionID</b>				
The transaction ID generated by the merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				
Response	Required	Alphanumeric	20	201508180000001

<b>Response.Amount</b>				
------------------------	--	--	--	--

A numeric value containing the total transaction amount ISO Formatted with no decimal point.  e.g. 1.00 USD received as 100 1.00 SAR received as 100 1.00 AED received as 100 1.000 JOD received as 1000				
Response	Required	Numeric	9	100

<b>Response.CurrencyISOCode</b>				
The numeric ISO Code for the currency and not the character value.  e.g. 840 for US Dollar 400 for JOD 682 for SAR 784 for AED				
Response	Required	Numeric	3	840

<b>Response.StatusDescription</b>				
Alphanumeric value representing a message describing the response status as received from SmartRoute using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Response	Required	Alphanumeric	100	Payment processed successfully

<b>Response.MerchantID</b>				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Response	Required	Alphanumeric	40	MID0001

<b>Response.MessageID</b>				
Alphanumeric value representing the action to be called, <b>4</b> for the refund transaction.				
Response	Required	Alphanumeric	2	3

<b>Response.RRN</b>				
Alphanumeric value representing a Receipt Reference Number as a reference for the current payment transaction. This value will be returned if the value is provided from the gateway.				
Response	Optional	Alphanumeric	60	2015082016004628400000000000

<b>Response.SecureHash</b>				
Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all response parameter appended in alphabetical order based on parameter's name, with no separators and no terminating character. Please refer to <a href="#">Appendix B: Secure Hash – Refund Transaction</a> for more details about secure hash generation.				

Response	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e
----------	----------	--------------	----	--

### 3.9. Recurring Payment

This message is intended to perform a recurring payment; where a payment is already performed with the customer (card holder) existing, then other payments are performed on behalf of the customer (card holder). It's based on the API communication model as described in [Communication Model](#) section.

#### 3.9.1. Request Fields: Basic Fields

Field Name				
Field Description				
Request/Response	Required/Optional	Field Type	Length	Sample Data

MessageID				
Alphanumeric value representing the action to be called, <b>11</b> for Recurring Payment				
Request	Required	Alphanumeric	2	11

TransactionID				
The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				
Request	Required	Alphanumeric	20	1440954863817

MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Request	Required	Alphanumeric	40	MID0001

Amount				
A numeric value containing the Item purchase amount ISO Formatted with no decimal point. e.g. 100 for 1.00 USD				
Request	Required	Numeric	9	100

CurrencyISOCode				
The numeric ISO Code for the currency and not the character value.  e.g. 840 for US Dollar 400 for JOD 682 for SAR 784 for AED				

Request	Required	Numeric	3	840
---------	----------	---------	---	-----

#### CardNumber

The customer's card number that will be used in the payment. This parameter is required if no token is present.

Request	Conditional	Numeric	19	4111111111111111
---------	-------------	---------	----	------------------

#### ExpiryDateYear

The customer's card expiry date year digits that will be used in the payment. The format of this parameter should be in the form (YY). This parameter is required if no token is present.

Request	Conditional	Numeric	2	17
---------	-------------	---------	---	----

#### ExpiryDateMonth

The customer's card expiry date month digits that will be used in the payment. The format of this parameter should be in the form (MM). This parameter is required if no token is present.

Request	Conditional	Numeric	2	02
---------	-------------	---------	---	----

#### ClientIPAddress

A value representing the client's public IP Address

Request	Required	Alphanumeric	19	79.183.118.122
---------	----------	--------------	----	----------------

#### PaymentDescription

Alphanumeric string containing a narrative description of the payment order using the language specified in the language parameter.  
This value should be UTF-8 encoded when it is entered into the secure hash generation process.

Request	Required	Alphanumeric	100	SamplePayment
---------	----------	--------------	-----	---------------

#### SecureHash

Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string starting with the merchant's Merchant Authentication Token, then all parameters(required parameters and optional parameters if they are provided) Ordered alphabetically by parameter's name should be part of the secure hash, with no separators and no terminating character.  
Please refer to [Appendix B: Secure Hash – Recurring Payment](#) for more details about secure hash generation

Request	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e
---------	----------	--------------	----	--

### 3.9.2. Response Fields: Basic Fields

Response.StatusCode				
Alphanumeric value representing the response code, this code covers errors generated by SmartRoute. Check <a href="#">Appendix A: Recurring Payment Response Codes</a> for descriptive details about Response Codes.				
Response	Required	Alphanumeric	5	00000

Response.StatusDescription				
Alphanumeric value representing a message describing the response status as received from SmartRoute using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Response	Required	Alphanumeric	100	Payment processed successfully

Response.Amount				
A numeric value containing the total transaction amount ISO Formatted with no decimal point.  e.g. 1.00 USD received as 100 1.00 SAR received as 100 1.00 AED received as 100 1.000 JOD received as 1000				
Response	Required	Numeric	9	100

Response.CurrencyISOCode				
The numeric ISO Code for the currency and not the character value.  e.g. 840 for US Dollar 400 for JOD 682 for SAR 784 for AED				
Response	Required	Numeric	3	840

Response.MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Response	Required	Alphanumeric	40	MID0001

Response.TransactionID				
The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				

Response	Required	Alphanumeric	20	201508180000001
----------	----------	--------------	----	-----------------

#### Response.MessageID

Alphanumeric value representing the action to be called, **11** for **Recurring Payment**

Response	Required	Alphanumeric	2	11
----------	----------	--------------	---	----

#### Response.SecureHash

Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string starting with the merchant's Merchant Authentication Token, then all response parameter appended in alphabetical order based on parameter's name, with no separators and no terminating character. Please refer to [Appendix B: Secure Hash – Recurring Payment](#) for more details about secure hash generation.

Response	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e
----------	----------	--------------	----	--

### 3.9.3. Other Optional Fields

#### CardHolderName

The customer's card holder name that will be used in the payment. This parameter is optional if no token is present. The format should be alphabetic with spaces allowed.

Request	Optional	Alphabetic	64	Card Holder Name
---------	----------	------------	----	------------------

#### ItemID

The custom item ID for the merchant.

Request	Optional	Alphanumeric	25	Item1
---------	----------	--------------	----	-------

#### Channel

The Channel to be used by SmartRoute System. It could be one of:

0 → E-Commerce,

1 → IVR

2 → POS

Request	Optional	Numeric	1	0
---------	----------	---------	---	---

#### Quantity

A numeric value greater than ZERO represents the quantity of purchased Item

Request	Optional	Numeric	5	1
---------	----------	---------	---	---

#### Version

A numeric value with (.) separator representing the version of the command to be used. Send it as 1.0.

Send it as 2.0 to:

1- Change Response.PaymentMethod format.

2- Add support for the RecurringSeriesID field.

Request	Optional	Numeric	5	1.0
---------	----------	---------	---	-----

FrameworkInfo				
An alphanumeric value representing the client's used framework.				
Request	Optional	Alphanumeric	30	Android 7.0

Token				
The token that will be used in this request; to represent a previously used card information. This parameter is a part of the tokenization parameters, check the Tokenization section for more details.				
Request	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27

RecurringSeriesID				
The series id that will be used in this request; to verify that the card information provided in the request fields was previously used in a payment transaction.				
This field is supported only if the Version field is set to 2.0				
Request	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27

Response.GatewayStatusCode				
Alphanumeric value representing the gateway response code, this code covers errors generated by the chosen gateway.				
Response	Optional	Alphanumeric	15	0000

Response.GatewayStatusDescription				
Alphanumeric value representing a message describing the response status as received from the chosen gateway using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Response	Optional	Alphanumeric	100	Sample Gateway Description

Response.GatewayName				
This value represents the gateway name that processed the transaction, it can be alphanumeric with some special characters like space, '@' and '_'.				
Response	Optional	Alphanumeric and Some Special	40	TestGateway

Response.RRN				
Alphanumeric value representing a Receipt Reference Number as a reference for the current payment transaction. This value will be returned if the value is provided from the gateway.				
Response	Optional	Alphanumeric	60	2015082016004628400000000000

Response.ApprovalCode				
Approval Code received from Payment Processor such as Visa. It will be returned only when the transaction is success. This value will be returned if the value is provided from the gateway.				
Response	Optional	Alphanumeric	10	12345678

Response.PaymentMethod				
<p>An Alphanumeric value to indicate which payment method will be used. Supported values depend on the requested <b>version</b> as follows:</p> <p><b>If Version is 1.0 :</b></p> <p>1 → that means a payment using Card. 2 → that means a payment using SADAD.</p> <p><b>If Version is 2.0 :</b></p> <p>1:Card Name (1 indicates Payment Method Card) e.g. 1:Visa 2 (indicates Payment Method SADAD).</p> <p>* Possible Card Names are provided by SmartRoute operation team upon merchant enrollment.</p>				
Request	Required	Alphanumeric	42	2

### 3.10. Completion Message

This message is intended to perform a Transaction completion. It's based on the Back-To-Back communication model as described in [Communication Model section](#).

#### 3.10.1. Request Fields

Field Name				
Field Description				
Request/Response	Required/Optional	Field Type	Length	Sample Data

MessageID				
Alphanumeric value representing the action to be called, <b>5</b> for the completion transaction.				
Request	Required	Alphanumeric	2	5

MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Request	Required	Alphanumeric	40	MID0001

TransactionID				
The transaction ID generated by the merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				
Request	Required	Alphanumeric	20	1440954863817

OriginalTransactionID				
The transaction ID of the original transaction, which is needed to refund it.				
Request	Required	Alphanumeric	20	1440594083737

Amount				
A numeric value containing the Item purchase amount ISO Formatted with no decimal point.  e.g. 100 for 1.00 USD				
Request	Required	Numeric	9	100

CurrencyISOCode				
The numeric ISO Code for the currency and not the character value.  e.g. 840 for US Dollar 400 for JOD 682 for SAR 784 for AED				
Request	Required	Numeric	3	840

Version				
A numeric value with (.) separator representing the version of the command to be used. Send it as 1.0				
Request	Optional	Numeric	5	1.0

SecureHash				
Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all parameters (required parameters and optional parameters if they are provided) ordered alphabetically by parameter's name should be part of the secure hash, with no separators and no terminating character. Please refer to <a href="#">Appendix B: Secure Hash – Refund Transaction Action</a> for more details about secure hash generation				
Request	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318 edc283bbbea27bc5d7bf7d a30f4f2e62b89df74a2e

### 3.10.2. Response Fields

Response.StatusCode				
Alphanumeric value representing the response code, this code covers errors generated by SmartRoute. Check <a href="#">Appendix A: Refund Response Codes</a> for descriptive details about Response Codes.				
Response	Required	Alphanumeric	5	00000

Response.OriginalTransactionID				
The transaction ID of the original transaction, which is needed to void it.				
Request	Required	Alphanumeric	20	1440594083737

Response.TransactionID				
The transaction ID generated by the merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.				
Response	Required	Alphanumeric	20	2015081800000001

Response.Amount				
A numeric value containing the total transaction amount ISO Formatted with no decimal point.  e.g. 1.00 USD received as 100 1.00 SAR received as 100 1.00 AED received as 100 1.000 JOD received as 1000				
Response	Required	Numeric	9	100

Response.CurrencyISOCode				
The numeric ISO Code for the currency and not the character value. e.g. 840 for US Dollar 400 for JOD 682 for SAR 784 for AED				
Response	Required	Numeric	3	840

Response.StatusDescription				
Alphanumeric value representing a message describing the response status as received from SmartRoute using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Response	Required	Alphanumeric	100	Payment processed successfully

Response.MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				
Response	Required	Alphanumeric	40	MID0001

Response.MessageID				
Alphanumeric value representing the action to be called, <b>4</b> for the refund transaction.				
Response	Required	Alphanumeric	2	3

Response.RRN				
Alphanumeric value representing a Receipt Reference Number as a reference for the current payment transaction. This value will be returned if the value is provided from the gateway.				
Response	Optional	Alphanumeric	60	2015082016004628400000000000

Response.SecureHash				
Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string <u>starting</u> with the merchant's Merchant Authentication Token, then all response parameter appended in alphabetical order based on parameter's name, with no separators and no terminating character. Please refer to <a href="#">Appendix B: Secure Hash – Refund Transaction</a> for more details about secure hash generation.				
Response	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e

## 4. Appendices

### 4.1. Appendix A: Response codes

#### 4.1.1. Redirect Payment Response codes

Table 1: Redirect Payment Response codes

Status Code	Description
00000	Transaction Successful.
00001	Merchant ID is missing
00002	Amount is missing
00003	Currency code is missing
00004	Message ID is missing
00005	Transaction ID is missing
00006	Quantity is missing
00007	Secure hash is missing
00008	Invalid amount
00009	Invalid currency code

00010	Invalid language
00011	Invalid message ID
00012	Invalid transaction ID
00013	Invalid response back URL
00014	Invalid quantity
00015	Merchant is not available
00016	Message is not available
00017	Duplicate transaction ID
00018	Secure hash doesn't match
00019	Abnormal error
00020	Message is not supported
00021	Original transaction ID is missing
00022	Invalid original transaction ID
00023	Original transaction is not found
00024	Original transaction requires reversal
00025	Channel is missing
00026	Invalid channel

00027	BIN couldn't be detected
00054	Double submission error. When you get this error, you should perform an inquiry to get the actual transaction status.
01111	Gateway Communication Error
10001	Payment Failed.
10002	Fraud Validation Error

#### 4.1.2. Direct Post Payment Response codes

**Table 2 : Direct Post (Sale) Response codes**

Status Code	Description
00000	Transaction Successful.
00001	Merchant ID is missing
00002	Amount is missing
00003	Currency code is missing
00004	Message ID is missing
00005	Transaction ID is missing
00006	Quantity is missing
00007	Secure hash is missing
00008	Invalid amount

00009	Invalid currency code
00010	Invalid language
00011	Invalid message ID
00012	Invalid transaction ID
00013	Invalid response back URL
00014	Invalid quantity
00015	Merchant is not available
00016	Message is not available
00017	Duplicate transaction ID
00018	Secure hash doesn't match
00019	Abnormal error
00020	Message is not supported
00021	Original transaction ID is missing
00022	Invalid original transaction ID
00023	Original transaction is not found
00024	Original transaction requires reversal
00025	Channel is missing

00026	Invalid channel
00027	BIN couldn't be detected
00028	Original transaction is already reversed
00029	Payment method is not supported
00030	No payment methods are supported
00031	Transaction Timeout
00032	No Payment Methods Received
00033	Invalid Payment Method
00034	Missing Expiry Date
00035	Missing Security Code
00036	Missing Card Number
00037	Invalid Expiry Date format
00038	Invalid Card Number
00039	Missing SADAD OLP ID
00040	Invalid Security Code
00054	Double submission error. When you get this error, you should perform an inquiry to get the actual transaction status.
01111	Gateway Communication Error

10001	Payment Failed.
10002	Fraud Validation Error

#### 4.1.3. Direct Post Verify Response codes

**Table 3 Direct Post Verify Response codes**

Status Code	Description
00000	Transaction Successful.
00001	Merchant ID is missing
00002	Amount is missing
00003	Currency code is missing
00004	Message ID is missing
00005	Transaction ID is missing
00006	Quantity is missing
00007	Secure hash is missing
00008	Invalid amount
00009	Invalid currency code

00010	Invalid language
00011	Invalid message ID
00012	Invalid transaction ID
00013	Invalid response back URL
00014	Invalid quantity
00015	Merchant is not available
00016	Message is not available
00017	Duplicate transaction ID
00018	Secure hash doesn't match
00019	Abnormal error
00020	Message is not supported
00021	Original transaction ID is missing
00022	Invalid original transaction ID
00023	Original transaction is not found
00024	Original transaction requires reversal
00025	Channel is missing
00026	Invalid channel

00027	BIN couldn't be detected
00028	Original transaction is already reversed
00029	Payment method is not supported
00030	No payment methods are supported
00031	Transaction Timeout
00032	No Payment Methods Received
00033	Invalid Payment Method
00034	Missing Expiry Date
00035	Missing Security Code
00036	Missing Card Number
00037	Invalid Expiry Date format
00038	Invalid Card Number
00039	Missing SADAD OLP ID
00040	Invalid Security Code
00054	Double submission error. When you get this error, you should perform an inquiry to get the actual transaction status.
01111	Gateway Communication Error
10001	Payment Failed.

10002	Fraud Validation Error
-------	------------------------

#### 4.1.4. API Payment Response codes

**Table 4 : API Payment Response codes**

Status Code	Description
00000	Transaction Successful.
00001	Merchant ID is missing
00002	Amount is missing
00003	Currency code is missing
00004	Message ID is missing
00005	Transaction ID is missing
00006	Quantity is missing
00007	Secure hash is missing
00008	Invalid amount
00009	Invalid currency code

00011	Invalid message ID
00012	Invalid transaction ID
00014	Invalid quantity
00015	Merchant is not available
00016	Message is not available
00017	Duplicate transaction ID
00018	Secure hash doesn't match
00019	Abnormal error
00020	Message is not supported
00026	Invalid channel
00027	BIN couldn't be detected
00029	Payment method is not supported
00030	No payment methods are supported
00031	Transaction Timeout
00032	No Payment Methods Received
00033	Invalid Payment Method
00034	Missing Expiry Date

00035	Missing Security Code
00036	Missing Card Number
00037	Invalid Expiry Date format
00038	Invalid Card Number
00039	Missing SADAD OLP ID
00040	Invalid Security Code
01111	Gateway Communication Error
10001	Payment Failed.
10002	Fraud Validation Error
20001	3D-Secure Authentication Required
20002	SADAD Authentication Required

#### 4.1.5. API mPayment Response codes

Table 5 : API mPayment Response codes

Status Code	Description
00000	Transaction Successful.
00001	Merchant ID is missing
00002	Amount is missing

00003	Currency code is missing
00004	Message ID is missing
00005	Transaction ID is missing
00006	Quantity is missing
00007	Secure hash is missing
00008	Invalid amount
00009	Invalid currency code
00011	Invalid message ID
00012	Invalid transaction ID
00014	Invalid quantity
00015	Merchant is not available
00016	Message is not available
00017	Duplicate transaction ID
00018	Secure hash doesn't match
00019	Abnormal error
00020	Message is not supported
00026	Invalid channel

00027	BIN couldn't be detected
00029	Payment method is not supported
00030	No payment methods are supported
00031	Transaction Timeout
00032	No Payment Methods Received
00033	Invalid Payment Method
00034	Missing Expiry Date
00035	Missing Security Code
00036	Missing Card Number
00037	Invalid Expiry Date format
00038	Invalid Card Number
00039	Missing SADAD OLP ID
00040	Invalid Security Code
01111	Gateway Communication Error
10001	Payment Failed.
10002	Fraud Validation Error
20002	SADAD Authentication Required

#### 4.1.6. API Approve Response codes

Table 6 : API Approve Response codes

Status Code	Description
00000	Transaction Successful.
00001	Merchant ID is missing
00004	Message ID is missing
00005	Transaction ID is missing
00007	Secure hash is missing
00011	Invalid message ID
00012	Invalid transaction ID
00015	Merchant is not available
00016	Message is not available
00018	Secure hash doesn't match
00019	Abnormal error

00020	Message is not supported
00029	Payment method is not supported
00030	No payment methods are supported
00031	Transaction Timeout
00032	No Payment Methods Received
00033	Invalid Payment Method
01111	Gateway Communication Error
10001	Payment Failed.
10002	Fraud Validation Error

#### 4.1.7. Transaction Inquiry Response Codes

**Table 7: Transaction Inquiry Response Codes**

Status Code	Description
00000	Transaction Successful.
00001	Merchant ID is missing
00004	Message ID is missing
00007	Secure hash is missing
00011	Invalid message ID

00015	Merchant is not available
00016	Message is not available
00018	Secure hash doesn't match
00019	Abnormal error
00020	Message is not supported
00021	Original transaction ID is missing
00022	Invalid original transaction ID
00023	Original transaction is not found
01111	Gateway Communication Error

#### 4.1.8. Refund Response Codes

**Table 8: Refund Response Codes**

Status Code	Description
00000	Transaction Successful.
00001	Merchant ID is missing
00002	Amount is missing
00003	Currency code is missing
00004	Message ID is missing

00005	Transaction ID is missing
00007	Secure hash is missing
00008	Invalid amount
00009	Invalid currency code
00011	Invalid message ID
00012	Invalid transaction ID
00015	Merchant is not available
00016	Message is not available
00017	Duplicate transaction ID
00018	Secure hash doesn't match
00019	Abnormal error
00020	Message is not supported
00021	Original transaction ID is missing
00022	Invalid original transaction ID
00023	Original transaction is not found
00024	Original transaction requires reversal
01111	Gateway Communication Error

40001	Refund failed.
-------	----------------

#### 4.1.9. Recurring Payment Response codes

Table 9 : Recurring Payment Response codes

Status Code	Description
00000	Transaction Successful.
00001	Merchant ID is missing
00002	Amount is missing
00003	Currency code is missing
00004	Message ID is missing
00005	Transaction ID is missing
00006	Quantity is missing
00007	Secure hash is missing
00008	Invalid amount
00009	Invalid currency code
00011	Invalid message ID

00012	Invalid transaction ID
00014	Invalid quantity
00015	Merchant is not available
00016	Message is not available
00017	Duplicate transaction ID
00018	Secure hash doesn't match
00019	Abnormal error
00020	Message is not supported
00026	Invalid channel
00027	BIN couldn't be detected
00029	Payment method is not supported
00030	No payment methods are supported
00031	Transaction Timeout
00032	No Payment Methods Received
00033	Invalid Payment Method
00034	Missing Expiry Date
00035	Missing Security Code

00036	Missing Card Number
00037	Invalid Expiry Date format
00038	Invalid Card Number
00039	Missing SADAD OLP ID
00040	Invalid Security Code
01111	Gateway Communication Error
10001	Payment Failed.
10002	Fraud Validation Error
20002	SADAD Authentication Required

## 4.2. Appendix B: Secure Hash

This section clarifies how secure hash must be generated using all required request parameters and optional parameters if they are provided.

Below examples show how to generate secure hash for each action type:

### 4.2.1. Redirect Payment

Table 10: Redirect Payment– Request message

**Input request parameters:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **MessageID:** 1
- **TransactionID:** 12345678901234567890
- **MerchantID:** STSPayOneM
- **Amount:** 100
- **Language:** En
- **CurrencyISOCode:** 400
- **PaymentDescription:** Sample Payment Description
- **ResponseBackURL:** https://MerchatWebSite/PaymentResponse.do
- **ThemeID:** theme1
- **Channel:** 0
- **Quantity:** 1
- **Version:** 1.0

**The order of parameters will be:**

Amount, Channel, CurrencyISOCode, Language, MerchantID, MessageID,  
PaymentDescription, Quantity, ResponseBackURL, ThemeID, TransactionID, Version

**The input to the Secure Hash generation routine would be:**

**Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly1000400EnSTSPayOneM1Sample+Payment+Description1https://MerchatWebSite/PaymentResponse.dotheme1123456789012345678901.0**

**Output:**

ddf2b07b95a3d93cc1ba6cd38dc69dbc1cf36819aa0bf83f549c827f98e6a84f

Table 11 Redirect Payment – Response message

**Input response message:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **Response.MessageID:** 1
- **Response.TransactionID:** 12345678901234567890
- **Response.StatusCode:** 00000
- **Response.StatusDescription:** Payment processed successfully
- **Response.GatewayStatusCode:** 0000
- **Response.GatewayName:** TestGateway
- **Response.GatewayStatusDescription:** Sample Gateway Description
- **Response.Amount:** 100
- **Response.ApprovalCode:** 654321
- **Response.CardExpiryDate:** 0416
- **Response.CardHolderName:** Card Holder
- **Response.CurrencyISOCode:** 400
- **Response.CardNumber:** 400555\*\*\*\*\*0001
- **Response.MerchantID:** STSPayOneM
- **Response.RRN:** 123456

**The order of parameters will be:**

Response.Amount, Response.ApprovalCode, Response.CardExpiryDate,  
Response.CardHolderName, Response.CardNumber, Response.CurrencyISOCode,  
Response.GatewayName, Response.GatewayStatusCode,  
Response.GatewayStatusDescription, Response.MerchantID, Response.MessageID,  
Response.RRN, Response.StatusCode, Response.StatusDescription, Response.TransactionID

**The input to the Secure Hash generation routine would be:**

**Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly1006543210416Card**  
**Holder400555\*\*\*\*\*0001400TestGateway0000Sample+Gateway+DescriptionSTSPayOneM11**  
**2345600000Payment+processed+successfully12345678901234567890**

**Output:**

46c8077b8fc7da3e53268c85b5a334678851a5ec6a84af3bc3d6f696e76ce8dd

#### 4.2.2. Direct Post Payment

Table 12 Direct Post Payment – Request message

**Input request parameters:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **MessageID:** 1
- **TransactionID:** 12345678901234567890
- **MerchantID:** STSPayOneM
- **Amount:** 100
- **Language:** En
- **PaymentMethod:** 1
- **CurrencyISOCode:** 400
- **PaymentDescription:** Sample Payment Description
- **ResponseBackURL:** <https://MerchatWebSite/PaymentResponse.do>
- **CardNumber:** 4111111111111111
- **ExpiryDateYear:** 22
- **ExpiryDateMonth:** 01
- **SecurityCode:** 854
- **CardHolderName:** Card Holder
- **Channel:** 0
- **Quantity:** 1
- **Version:** 1.0

**The order of parameters will be:**

Amount, Channel, CurrencyISOCode, Language, MerchantID, MessageID,  
PaymentDescription, PaymentMethod, Quantity, ResponseBackURL, TransactionID, Version

**The input to the Secure Hash generation routine would be:**

**Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly1000400EnSTSPayOneM1Sample+Payment+Description11<https://MerchatWebSite/PaymentResponse.do>123456789012345678901.0**

**Output:**

3e6a7361eccc30e0a9813f3ee90b845d8dcf4d69564ef2ec64fb809bc8591481

**Note:** CardNumber, ExpiryDateYear, ExpiryDateMonth, SecurityCode and CardHolderName are not a part of the Secure Hash.

**Table 13: Direct Post Payment – Response message**

**Input response message:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **Response.MessageID:** 1
- **Response.TransactionID:** 12345678901234567890
- **Response.StatusCode:** 00000
- **Response.StatusDescription:** Payment processed successfully
- **Response.GatewayStatusCode:** 0000
- **Response.GatewayStatusDescription:** Sample Gateway Description
- **Response.GatewayName:** TestGateway
- **Response.Amount:** 100
- **Response.ApprovalCode:** 654321
- **Response.CardExpiryDate:** 0122
- **Response.CardHolderName:** Card Holder
- **Response.CurrencyISOCode:** 400
- **Response.CardNumber:** 411111\*\*\*\*\*1111
- **Response.MerchantID:** STSPayOneM
- **Response.RRN:** 123456

**The order of parameters will be:**

Response.Amount, Response.ApprovalCode, Response.CardExpiryDate,  
Response.CardHolderName, Response.CardNumber, Response.CurrencyISOCode,  
Response.GatewayName, Response.GatewayStatusCode,  
Response.GatewayStatusDescription, Response.MerchantID, Response.MessageID ,  
Response.RRN, Response.StatusCode, Response.StatusDescription, Response.TransactionID

**The input to the Secure Hash generation routine would be:**

**Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly1006543210122Card**  
**Holder411111\*\*\*\*\*1111400TestGateway0000Sample+Gateway+DescriptionSTSPayOneM11**  
**2345600000Payment+processed+successfully12345678901234567890**

**Output:**

e801dccf0e59fa56517576d10e51a8b6bd5f56c3f14d67c0c446fc10c3a65031

#### 4.2.3. Direct Post Verify

Table 14 Direct Post Verify – Request message

**Input request parameters:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **MessageID:** 12
- **TransactionID:** 12345678901234567890
- **MerchantID:** STSPayOneM
- **Amount:** 100
- **Language:** En
- **PaymentMethod:** 1
- **CurrencyISOCode:** 400
- **PaymentDescription:** Sample Payment Description
- **ResponseBackURL:** <https://MerchatWebSite/PaymentResponse.do>
- **CardNumber:** 4111111111111111
- **ExpiryDateYear:** 22
- **ExpiryDateMonth:** 01
- **SecurityCode:** 854
- **CardHolderName:** Card Holder
- **Channel:** 0
- **Quantity:** 1
- **Version:** 1.0

**The order of parameters will be:**

Amount, Channel, CurrencyISOCode, Language, MerchantID, MessageID,  
PaymentDescription, PaymentMethod, Quantity, ResponseBackURL, TransactionID, Version

**The input to the Secure Hash generation routine would be:**

**Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly1000400EnSTSPayOneM12Sample+Payment+Description11<https://MerchatWebSite/PaymentResponse.do>123456789012345678901.0**

**Output:**

92c3205bb9002cbc654311befbdd0cf3f41011bbbfa52da5604145604218d1a3

**Note:** CardNumber, ExpiryDateYear, ExpiryDateMonth, SecurityCode and CardHolderName are not a part of the Secure Hash.

Table 15 Direct Post Verify – Response message

**Input response message:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **Response.MessageID:** 12
- **Response.TransactionID:** 12345678901234567890
- **Response.StatusCode:** 00000
- **Response.StatusDescription:** Payment processed successfully
- **Response.GatewayStatusCode:** 0000
- **Response.GatewayStatusDescription:** Sample Gateway Description
- **Response.GatewayName:** TestGateway
- **Response.Amount:** 100
- **Response.ApprovalCode:** 654321
- **Response.CardExpiryDate:** 0122
- **Response.CardHolderName:** Card Holder
- **Response.CurrencyISOCode:** 400
- **Response.CardNumber:** 411111\*\*\*\*\*1111
- **Response.MerchantID:** STSPayOneM
- **Response.RRN:** 123456

**The order of parameters will be:**

Response.Amount, Response.ApprovalCode, Response.CardExpiryDate,  
Response.CardHolderName, Response.CardNumber, Response.CurrencyISOCode,  
Response.GatewayName, Response.GatewayStatusCode,  
Response.GatewayStatusDescription, Response.MerchantID, Response.MessageID ,  
Response.RRN, Response.StatusCode, Response.StatusDescription, Response.TransactionID

**The input to the Secure Hash generation routine would be:**

**Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly1006543210122Card**  
**Holder411111\*\*\*\*\*1111400TestGateway0000Sample+Gateway+DescriptionSTSPayOneM12**  
**12345600000Payment+processed+successfully12345678901234567890**

**Output:**

80bdc4dc376d5402d93ed3858b688ce4171f23b8d38692c3a814f9de4b56c8cf

#### 4.2.4. API Payment

Table 16 API Payment – Request message

##### Input request parameters:

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **MessageID:** 8
- **TransactionID:** 12345678901234567890
- **MerchantID:** STSPayOneM
- **Amount:** 2000
- **PaymentMethod:** 1
- **CurrencyISOCode:** 840
- **CardNumber:** 4111111111111111
- **ExpiryDateYear:** 22
- **ExpiryDateMonth:** 01
- **SecurityCode:** 854
- **PaymentDescription:** Sample Payment
- **ClientIPAddress:** 188.888.50.125

##### The order of parameters will be:

Amount, CardNumber, ClientIPAddress, CurrencyISOCode, ExpiryDateMonth, ExpiryDateYear, MerchantID, MessageID, PaymentDescription, PaymentMethod, SecurityCode, TransactionID

##### The input to the Secure Hash generation routine would be:

**Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly20004111111111111111188.888.50.1258400122STSPayOneM8Sample+Payment185412345678901234567890**

##### Output:

b6e4b31d5581d91d3b1022b3efb33ccfbbe5b7e7bd17dcaa9aa6beceb42b444

Table 17 API Payment – Response message

**Input response message:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **Response.MessageID:** 8
- **Response.TransactionID:** 12345678901234567890
- **Response.StatusCode:** 20001
- **Response.StatusDescription:** 3D-Secure Authentication Required
- **Response.GatewayStatusCode:** 8005
- **Response.GatewayName:** TestGateway
- **Response.Amount:** 2000
- **Response.CurrencyISOCode:** 840
- **Response.MerchantID:** STSPayOneM
- **Response.PaymentMethod:** 1
- **Response.AuthenticationURL:** https://dropit.3dsecure.net
- **Response.PaReq:** eJxVUttu4jAQ/ZWqH4AvJCxBgyVlkJo

**The order of parameters will be:**

Response.Amount, Response.AuthenticationURL, Response.CurrencyISOCode,  
Response.GatewayName, Response.GatewayStatusCode, Response.MerchantID,  
Response.MessageID, Response.PaReq, Response.PaymentMethod, Response.StatusCode,  
Response.StatusDescription, Response.TransactionID

**The input to the Secure Hash generation routine would be:**

Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly2000https://dropit.3dsecure.net840TestGateway  
8005STSPayOneMeJxVUttu4jAQ/ZWqH4AvJCxBgyVlkJo1200013D-  
Secure+Authentication+Required12345678901234567890

**Output:**

9af4f51d3ba17fdc1658350ff9782167e8c6fcac3619e88c5d2d9a1ce0bd6f63

#### 4.2.5. API mPayment

Table 18 API mPayment – Request message

**Input request parameters:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **MessageID:** 9
- **TransactionID:** 12345678901234567890
- **MerchantID:** STSPayOneM
- **Amount:** 2000
- **PaymentMethod:** 1
- **CurrencyISOCode:** 840
- **CardNumber:** 4111111111111111
- **ExpiryDateYear:** 22
- **ExpiryDateMonth:** 01
- **SecurityCode:** 854
- **PaymentDescription:** Sample Payment
- **ClientIPaddress:** 188.888.50.125

**The order of parameters will be:**

Amount, CardNumber, ClientIPaddress, CurrencyISOCode, ExpiryDateMonth,  
ExpiryDateYear, MerchantID, MessageID, PaymentDescription, PaymentMethod,  
SecurityCode, TransactionID

**The input to the Secure Hash generation routine would be:**

**Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly20004111111111111111188.888.50.1258400122ST  
SPayOneM9Sample+Payment185412345678901234567890**

**Output:**

899f3b541f659fc2c1e2254905d6beb640189dd0af5f46fa50139afc485a9ebc

Table 19 API mPayment – Response message

**Input response message:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **Response.MessageID:** 9
- **Response.TransactionID:** 12345678901234567890
- **Response.StatusCode:** 00000
- **Response.StatusDescription:** Payment processed successfully
- **Response.GatewayStatusCode:** 0000
- **Response.GatewayName:** TestGateway
- **Response.Amount:** 2000
- **Response.CurrencyISOCode:** 840
- **Response.MerchantID:** STSPayOneM
- **Response.PaymentMethod:** 1

**The order of parameters will be:**

Response.Amount, Response.CurrencyISOCode, Response.GatewayName,  
Response.GatewayStatusCode, Response.MerchantID, Response.MessageID,  
Response.PaymentMethod, Response.StatusCode, Response.StatusDescription,  
Response.TransactionID

**The input to the Secure Hash generation routine would be:**

**Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly2000840TestGateway0000STSPayOneM9100000**  
**Payment+processed+successfully12345678901234567890**

**Output:**

0c14aaf3a5bf8ca4c93b79cde4e91b8627bdcee34cffbe2f38a0e803b8fde862

#### 4.2.6. API Approve

Table 20 API Approve – Request message

##### Input request parameters:

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **MessageID:** 10
- **TransactionID:** 12345678901234567890
- **MerchantID:** STSPayOneM
- **estn:**  
cmdWd0xLS0dUU2JrZjJDTUhzczNKYXpPNUhCaGhuM1BITzYyUXZnTDZSMVNLQjk4NW9KOHVqYmhBZmM4ZWVKZS9mSGNmYyYtVXhxUUUVaY2xSendDSU9SMDFoRmZ3eUI4MXBURXV5OSStaU21VbVV5b3crODZKZzZ1VldmbVFHeWU2UTFSZ1R4WHp4L1g3OG1ueHo4cVZDSWF5Rlp5VFFyUWNqVzFZenAvbkttYVpac3NsVDFWM0FIUFR3MllLeE16RFdLQ0thbWIZVktS2VEeE5HcysrN2JTYWo4MklCRUhmc1IRdXRtU1VOak0yWm05ODFDeUdNRUITTmxQOFROVIZYL25VTmkzUXUxWGxjeStoODdkRUF4amlhRTJTUml2R2VyT0NScE5WT01zKzlienHEYnFQcW5kNVY0THI4VytE5OZ0t5VWNQR0h0ZDRDN2tOWTV3PT0=
- **PaymentMethod:** 2

##### The order of parameters will be:

MerchantID, MessageID, PaymentMethod, TransactionID, estn

##### The input to the Secure Hash generation routine would be:

**Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2lySTSPayOneM10212345678901234567890**  
cmdWd0xLS0dUU2JrZjJDTUhzczNKYXpPNUhCaGhuM1BITzYyUXZnTDZSMVNLQjk4NW9KOHVqYmhBZmM4ZWVKZS9mSGNmYyYtVXhxUUUVaY2xSendDSU9SMDFoRmZ3eUI4MXBURXV5OSStaU21VbVV5b3crODZKZzZ1VldmbVFHeWU2UTFSZ1R4WHp4L1g3OG1ueHo4cVZDSWF5Rlp5VFFyUWNqVzFZenAvbkttYVpac3NsVDFWM0FIUFR3MllLeE16RFdLQ0thbWIZVktS2VEeE5HcysrN2JTYWo4MklCRUhmc1IRdXRtU1VOak0yWm05ODFDeUdNRUITTmxQOFROVIZYL25VTmkzUXUxWGxjeStoODdkRUF4amlhRTJTUml2R2VyT0NScE5WT01zKzlienHEYnFQcW5kNVY0THI4VytE5OZ0t5VWNQR0h0ZDRDN2tOWTV3PT0=

##### Output:

460bd68a6c0a020408b55f3751184f39e9c537914d45b586f5960c1a1d3a66fe

Table 21 API Approve – Response message

**Input response message:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **Response.MessageID:** 10
- **Response.TransactionID:** 12345678901234567890
- **Response.StatusCode:** 00000
- **Response.StatusDescription:** Payment processed successfully
- **Response.GatewayStatusCode:** 0000
- **Response.GatewayName:** TestGateway
- **Response.Amount:** 2000
- **Response.CurrencyISOCode:** 840
- **Response.MerchantID:** STSPayOneM

**The order of parameters will be:**

Response.Amount, Response.CurrencyISOCode, Response.GatewayName,  
Response.GatewayStatusCode, Response.MerchantID, Response.MessageID,  
Response.StatusCode, Response.StatusDescription, Response.TransactionID

**The input to the Secure Hash generation routine would be:**

Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly2000840TestGateway0000STSPayOneM1000000Payment+processed+successfully12345678901234567890

**Output:**

b8289e077922b40d382cd2275354d845811bc25f6ca13ea8d45420e3f5100229

#### 4.2.7. Transaction Inquiry

Table 22 Transaction Inquiry - Request message

**Input request parameters:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **MessageID:** 2
- **MerchantID:** STSPayOneM
- **OriginalTransactionID:** 12345678901234567890
- **Version:** 1.0

**The order of parameters will be:**

MerchantID, MessageID, OriginalTransactionID, Version

**The input to the Secure Hash generation routine would be:**

Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2lySTSPayOneM2123456789012345678901.0

**Output:**

74012d2538c65ab3b03a50f665828a99a6e5eb574049a9930495d062b4bfb9fc

Table 23 Transaction Inquiry - Response message

**Input response message:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2Iy
- **Response.MessageID:** 2
- **Response.TransactionID:** 12345678901234567890
- **Response.StatusCode:** 00000
- **Response.StatusDescription:** Payment processed successfully
- **Response.GatewayStatusCode:** 0000
- **Response.GatewayStatusDescription:** Sample Gateway Description
- **Response.GatewayName:** TestGateway
- **Response.Amount:** 100
- **Response.ApprovalCode:** 654321
- **Response.CardExpiryDate:** 0416
- **Response.CardHolderName:** Card Holder
- **Response.CurrencyISOCode:** 400
- **Response.CardNumber:** 400555\*\*\*\*\*0001
- **Response.Token:** 17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27
- **Response.MerchantID:** STSPayOneM
- **Response.RRN:** 123456
- **Response.MessageStatus:** 00000
- **Response.ReversalStatus:** 1

**The order of parameters will be:**

Response.Amount, Response.ApprovalCode, Response.CardExpiryDate,  
Response.CardHolderName, Response.CardNumber, Response.CurrencyISOCode,  
Response.GatewayName, Response.GatewayStatusCode,  
Response.GatewayStatusDescription, Response.MerchantID, Response.MessageID,  
Response.MessageStatus, Response.RRN, Response.ReversalStatus, Response.StatusCode,  
Response.StatusDescription, Response.TransactionID, Response.Token

**The input to the Secure Hash generation routine would be:**

**Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2Iy1006543210416Card**  
**Holder400555\*\*\*\*\*0001400TestGateway0000Sample+Gateway+DescriptionSTSPayOneM20**  
**0000123456100000Payment+processed+successfully1234567890123456789017b61316feafe**  
**09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27**

**Output:**

d3b26346020922eb8d038e5f4902e8a110e529c81b0d29c3ff2989ddc575ec49

#### 4.2.8. Refund Transaction

Table 24 Refund Transaction - Request message

**Input request parameters:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **MessageID:** 4
- **MerchantID:** STSPayOneM
- **TransactionID:** 12345678901234567891
- **OriginalTransactionID:** 12345678901234567890
- **Amount:** 100
- **CurrencyISOCode:** 400
- **Version:** 1.0

**The order of parameters will be:**

Amount, CurrencyISOCode, MerchantID, MessageID, OriginalTransactionID, TransactionID, Version

**The input to the Secure Hash generation routine would be:**

Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly100400STSPayOneM4123456789012345678901234567890123456789012345678911.0

**Output:**

662e268fa5a3bcb255cab69261d6a950e3a225589d71b029ff6b6eafcb6c313e

Table 25 Refund Transaction - Response message

**Input response message:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **Response.StatusCode:** 0000
- **Response.OriginalTransactionID:** 12345678901234567890
- **Response.TransactionID:** 12345678901234567891
- **Response.Amount:** 100
- **Response.CurrencyISOCode:** 400
- **Response.StatusDescription:** Payment processed successfully
- **Response.MerchantID:** STSPayOneM
- **Response.MessageID:** 4
- **Response.RRN:** 123456

**The order of parameters will be:**

Response.Amount, Response.CurrencyISOCode, Response.MerchantID,  
Response.MessageID, Response.OriginalTransactionID, Response.RRN,  
Response.StatusCode, Response.StatusDescription, Response.TransactionID

**The input to the Secure Hash generation routine would be:**

Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly100400STSPayOneM4123456789012345678901234560000Payment+processed+successfully12345678901234567891

**Output:**

ef85cce7db5b4e0da8b1906781f06b522978223e7597a41abdbd818c0047d018

#### 4.2.9. Recurring Payment

Table 26 Recurring Payment – Request message

**Input request parameters:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **MessageID:** 11
- **TransactionID:** 12345678901234567890
- **MerchantID:** STSPayOneM
- **Amount:** 2000
- **CurrencyISOCode:** 840
- **CardNumber:** 4111111111111111
- **ExpiryDateYear:** 22
- **ExpiryDateMonth:** 01
- **PaymentDescription:** Sample Payment
- **ClientIPAddress:** 188.888.50.125
- **RecurringSeriesId:** 17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27

**The order of parameters will be:**

Amount, CardNumber, ClientIPAddress, CurrencyISOCode, ExpiryDateMonth, ExpiryDateYear, MerchantID, MessageID, PaymentDescription, RecurringSeriesId , TransactionID

**The input to the Secure Hash generation routine would be:**

**Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly20004111111111111111188.888.50.1258400122STSPayOneM11Sample+Payment17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e2712345678901234567890**

**Output:**

bedbe29fe3af2c6f54ec3c01bd01fedffbdffac2b11b72e106fb12009bc39ad0

Table 27 Recurring Payment – Response message

**Input response message:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **Response.MessageID:** 11
- **Response.TransactionID:** 12345678901234567890
- **Response.StatusCode:** 00000
- **Response.StatusDescription:** Payment processed successfully
- **Response.GatewayStatusCode:** 0000
- **Response.GatewayName:** TestGateway
- **Response.Amount:** 2000
- **Response.CurrencyISOCode:** 840
- **Response.MerchantID:** STSPayOneM

**The order of parameters will be:**

Response.Amount, Response.CurrencyISOCode, Response.GatewayName,  
Response.GatewayStatusCode, Response.MerchantID, Response.MessageID,  
Response.StatusCode, Response.StatusDescription, Response.TransactionID

**The input to the Secure Hash generation routine would be:**

Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly2000840TestGateway0000STSPayOneM1100000Payment+processed+successfully12345678901234567890

**Output:**

d67a2a1d25d62ca0e30b4e6c52700cd27af19845b426c1035b9327ebf3af4c24

#### 4.2.10. Completion Transaction

Table 28 Completion Transaction - Request message

**Input request parameters:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **MessageID:** 5
- **MerchantID:** STSPayOneM
- **TransactionID:** 12345678901234567891
- **OriginalTransactionID:** 12345678901234567890
- **Amount:** 100
- **CurrencyISOCode:** 400
- **Version:** 1.0

**The order of parameters will be:**

Amount, CurrencyISOCode, MerchantID, MessageID, OriginalTransactionID, TransactionID, Version

**The input to the Secure Hash generation routine would be:**

Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly100400STSPayOneM512345678901234567890123456789012345678911.0

**Output:**

e11d91e543dfc895f1d5580d6c6dcd671614dd6eb8a524953e273148d7a74046

Table 29 Completion Transaction - Response message

**Input response message:**

- **Merchant Authentication Token:** Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly
- **Response.StatusCode:** 0000
- **Response.OriginalTransactionID:** 12345678901234567890
- **Response.TransactionID:** 12345678901234567891
- **Response.Amount:** 100
- **Response.CurrencyISOCode:** 400
- **Response.StatusDescription:** Payment processed successfully
- **Response.MerchantID:** STSPayOneM
- **Response.MessageID:** 5
- **Response.RRN:** 123456

**The order of parameters will be:**

Response.Amount, Response.CurrencyISOCode, Response.MerchantID,  
Response.MessageID, Response.OriginalTransactionID, Response.RRN,  
Response.StatusCode, Response.StatusDescription, Response.TransactionID

**The input to the Secure Hash generation routine would be:**

Y2ExNzE2NDBlZjEyNmZhZjRmMmRmY2ly100400STSPayOneM5123456789012345678901234560000Payment+processed+successfully12345678901234567891

**Output:**

a56480422dd00a3230b3959d55a8732ca80148429ebc0a98109e2650ee77438d

### 4.3. Appendix C: Update Notification Message

This message is intended to send the payment response using SmartRoute interface. It's based on the API communication model as described in [Communication Model section](#). This message will be sent from SmartRoute to the merchant only if the merchant has the "Merchant Notification URL" filled, it slightly differs from the normal messages as it consists of a response only, not a request and a response, the response received will be the same like the payment response that will be received in the final step of the redirect payment.

#### 4.3.1. Response Fields: Basic Fields

Response.StatusCode				
Alphanumeric value representing the response code, this code covers errors generated by SmartRoute. Check <a href="#">Appendix A: Redirect Payment Response Codes</a> for descriptive details about Response Codes. Note that the update notification response codes are the same as the redirect payment response codes.				
Response	Required	Alphanumeric	5	00000

Response.StatusDescription				
Alphanumeric value representing a message describing the response status as received from SmartRoute using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.				
Response	Required	Alphanumeric	100	Payment processed successfully

Response.Amount				
A numeric value containing the total transaction amount ISO Formatted with no decimal point.  e.g. 1.00 USD received as 100 1.00 SAR received as 100 1.00 AED received as 100 1.000 JOD received as 1000				
Response	Required	Numeric	9	100

Response.CurrencyISOCode				
The numeric ISO Code for the currency and not the character value.  e.g. 840 for US Dollar				
Response	Required	Numeric	3	840

Response.MerchantID				
Alphanumeric value representing the unique ID of the merchant at SmartRoute, this value is provided by SmartRoute operation team upon merchant enrollment.				

Response	Required	Alphanumeric	40	MID0001
----------	----------	--------------	----	---------

#### Response.TransactionID

The Transaction ID generated by the Merchant, it represents a unique identifier for the transaction, and it is alphanumeric. It can't include special characters neither spaces.

Response	Required	Alphanumeric	20	201508180000001
----------	----------	--------------	----	-----------------

#### Response.MessageID

Alphanumeric value representing the action to be called, **1** for Sale

Response	Required	Alphanumeric	2	1
----------	----------	--------------	---	---

#### Response.SecureHash

Alphanumeric value representing generated hex-encoded hash using hashing algorithm SHA-2 (256), by concatenating parameters as a single string starting with the merchant's Merchant Authentication Token, then all response parameter appended in alphabetical order based on parameter's name, with no separators and no terminating character. Please refer to [Appendix B: Secure Hash – Redirect Payment \(Sale\)](#) for more details about secure hash generation. Note that the update notification secure hash is the same as the redirect payment response secure hash.

Response	Required	Alphanumeric	64	e9fbb3c46ec9c7dec2a318edc283bbbea27bc5d7bf7da30f4f2e62b89df74a2e
----------	----------	--------------	----	--

### 4.3.2. Other Optional Fields

#### Response.CardExpiryDate

Expiry date of the card (MMYY).

Response	Optional	Alphanumeric	4	0416
----------	----------	--------------	---	------

#### Response.CardHolderName

Card Holder Name

Response	Optional	Alphanumeric	32	FName LName
----------	----------	--------------	----	-------------

#### Response.CardNumber

Masked Card Number

Response	Optional	Alphanumeric	19	4747*****123
----------	----------	--------------	----	--------------

#### Response.GatewayStatusCode

Alphanumeric value representing the gateway response code, this code covers errors generated by the chosen gateway.

Response	Optional	Alphanumeric	15	0000
----------	----------	--------------	----	------

#### Response.GatewayStatusDescription

Alphanumeric value representing a message describing the response status as received from the chosen gateway using the language specified in the request; this parameter will be filled only after a complete execution process. This value should be UTF-8 encoded when it is entered into the secure hash generation process.

Response	Optional	Alphanumeric	100	Sample Gateway Description
----------	----------	--------------	-----	----------------------------

#### Response.GatewayName

This value represents the gateway name that processed the transaction, it can be alphanumeric with some special characters like space, '@' and '\_'.

Response	Optional	Alphanumeric and Some Special	40	TestGateway
----------	----------	-------------------------------	----	-------------

#### Response.RRN

Alphanumeric value representing a Receipt Reference Number as a reference for the current payment transaction. This value will be returned if the value is provided from the gateway.

Response	Optional	Alphanumeric	60	2015082016004628400000000000
----------	----------	--------------	----	------------------------------

#### Response.ApprovalCode

Approval Code received from Payment Processor such as Visa. It will be returned only when the transaction is successful. This value will be returned if the value is provided from the gateway.

Response	Optional	Alphanumeric	10	12345678
----------	----------	--------------	----	----------

#### Response.Token

The token that is assigned to the entered card information; responding to a "GenerateToken" flag with the value "Yes". This parameter is a part of the tokenization parameters, check the [Tokenization](#) section for more details.

Response	Optional	Alphanumeric	64	17b61316feafe09feb806ce33cdbfc85aed1b4173ed604f8fd5fa3cf72a02e27
----------	----------	--------------	----	--

## 4.4. Appendix D: 3D-Secure Implementation

If the “Response.StatusCode” in an **API Payment** was returned as 20001 then the merchant must proceed with 3DS authentication as follows (Steps from 1 to 5)

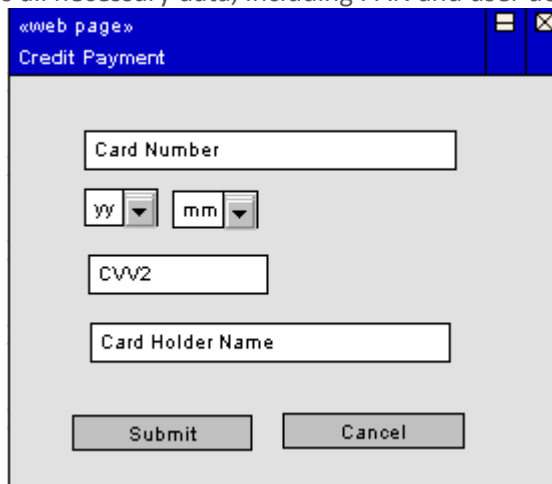
- **What is 3D-Secure:**

The 3-D Secure™ protocol was developed by Visa to improve the security of Internet payments. It is designed to allow authentication of cardholders by their Issuers at participating merchants. The objective is to benefit all participants by providing Issuers the ability to fully authenticate cardholders during an online purchase, reducing the likelihood of fraudulent usage of Visa cards and improving overall transaction performance.

- **How it works:**

**Step 1:**

Shopper browses at merchant site, adds items to shopping cart, then finalizes purchase. Merchant now has all necessary data, including PAN and user device information.

A screenshot of a web browser window showing a credit payment form. The window title is "Credit Payment". The form contains the following fields: "Card Number" (a text input), "yy" (a dropdown menu for year), "mm" (a dropdown menu for month), "CVV2" (a text input), and "Card Holder Name" (a text input). At the bottom of the form are two buttons: "Submit" and "Cancel".

**Step 2:**

The merchant sends the information to SmartRoute, in turn SmartRoute verifies if the card holder is enrolled into VISA 3DS directory service, if so it will send back to the merchant the response. Some of these parameters are:

- Response.PaReq
- Response.AuthenticationURL

The merchant will use “Response.AuthenticationURL” to popup or redirect the user to the issuer URL (Response.AuthenticationURL) where the card holder must authenticate his/her payment request. Also, the merchant receives additional field “Response.PaReq” which is the Payment Authentication Request received from SmartRoute

Step 3:

The merchant then constructs a page requesting the user to authenticate his payment request.



The following are mandatory fields which must be contained in the form (Authenticate)

```
<form name="AutoSubmitForm" action="<%= Response. AuthenticationURL %>"
method="POST">
<input type="hidden" name="PaReq" value="<%=Response.PaReq%>">
<input type="hidden" name="TermUrl" value="<%=
response.encodeUrl("https://merchant-return-URL")%>">
<input type="hidden" name="MD" value="echo">
<INPUT name="submit" value="Authenticate" type="submit" >
</form>
```

Where:

**Response.AuthenticationURL:** is returned by SmartRoute

**Response.PaReq** is returned by SmartRoute

**TermUrl** is the merchant site URL where to receive the authentication result from issuer side.

**MD** any value the merchant wishes to put like (Payment Unique Number) for example.

Step 4:

An authentication screen will be displayed as of the following:

The screenshot shows a web browser window with a blue title bar that reads «web page» and 3DS Issuer Authentication process. Inside the browser, there is a large text area containing the following XML snippet:

```
<?xml version="1.0" encoding="UTF-8"?><ThreeDSecure><Message id="msg.61"><PARES id="1639497"><version>1.0.2</version><Merchant><acqBIN>404949</acqBIN><merID>000000000271999
```

Below the text area is a button labeled "Submit".

This form is generated by the issuer of the card which contains the following

<FORM NAME="postPARESToMPIForm" ACTION="https://merchant-return-URL" METHOD="post">

<INPUT TYPE="hidden" NAME="PaRes"

VALUE="eJy1V1m3ojwW/Su1bj+6qgBFxVpevxUGETQoo+AbMyiDTDL8+o56p75dD193r+bFsm3ZOTvZJyHLv7o0+XHzyyrOs9cX4hf+8sPP3NyLs/D1RdfWP6mXv1ZLLSp9n1V9tyn91RL6VWWH/o/Ye31Jq/AXgRMvq+UBKH71wljZbLxTFMLeiFeI99d4ib2/IobSjeysXi1tt6AFaUXi5IJcLLG312XqlwK7wt+f8ZxYLNdfT3iJfcYfmnurQl1sbdKQp9w9+GgHI/eonGZ9sRmfMjRQBZel9i9x9Kza381xvE5PiemPwj8N0n+JvAl9sCX1zsdSPMGceN3+CuwRPJLNDv9iiLRXx9vS7+75pmPeiCNH+0l9pnb1c4+xaCHIAjU9Y4uNXO1rOP0S0449Xs6/U0QS+yBL6varptqZS2xt9bStW+3FQC AAF2ePkUulZ70IbTWKXg+SOujy9J34xU+RUmh30cUSMK8jOsovaf6r8ASu6eCPZZxtVTjMEO Dlf4PZJCsen2J6vr6G8Patv3VTn7IZYihhHEMX2Cog1ff4T9enIG+J2RB/h+FMXaWZ7FrJ/Fg18g g0K+j3PvxkdufaDTlzkRgCsF8RFQ/XYLMft4RfEJMESf2Z9Ivyv7OKN+TLsv7ZxXZd79j34hWS8 UP/Lsj/B+6lry+/OOzDtG49Kv6vxnwfbCvDO98hp00/iq8jk7zxJgpRjEB072lbXzCHINMxXGv73 HPnkvsl8O39J9r9WVOnh3lrRWdINxOtV4pb765G+308bg0HFpNKVGjBa6czL22Yjb2SOYtGp 5kY+l7zYKtJtU8qeRmE1T1DfekKTkzpWGW464fNxVNQc6IKrd1kz4mvNYJym4SsDK3LnFDyP SbB5w+x4zDbVKLB05r0mxEp64VZtl0di1hoFLHTNET8almt+KCzd17WX9Lfrn1+6cqc4ovWLu 2ny3GL+s4QIZAdQ4FgTFZhgHuMQStQINQ0H07auCtGmJ9LlbUNs8w7gz2hmFuuZaVLXGbn 4To5koApUvLoD2cuR0EFx4QOkdHkDEM2HEs2NOhZNAg12hcitx0fbFM2LEs2D7xSgMELRos d4AAf8SCDvlun+C7oxRBmjRZDUwgy7V7lpvAQe4gkd8x8hvWhpbcmMQMQn7yWBHJDg3LV MrLFGrlscK2oH7+MQ6NxZNMYPD5poEq1u2e/LdefjqohoUVNGo83eiddd4/Zx0VjHnTTHRu+l yfmk0rQ7kW7WOllQ/M05cxIE1YOX6dCiXhJN1jgT0vq7pr06Nsb2kQz1dBHbx+nIzApteKK+z yWN5pINLRxAgRdBztMAFmzit0wjgFvv7Av2cuRZsj2BLlif60NnYkPGiv1ZMndzMcvptDZmPf

```

DFytlzlj4TmPh0YQS7jgQv2DJlez4StrWfz8w5mVUixTNKu7nsZ9SoY+a5vrYCI1gUs3G6z8IZJfv
sebJXYEvFkQWr/hBnvRWN/JoMJwAymWtMRC6uRjDm/PgGQkgDwJ/v6w5Be9fucS1HY63
MQAD+5BukIQNGRUohRiim6W2vi77Np+QajP3DGLMHAKw8q1tbe6EYVEVczGxqTtH5gpm
NPHAolbaZ41sn94KderhgMb2Fli24cHrO56PaGDdT/TqSp5uWuh72HdPqF8X3ThyYIZ6ilolRh
GF2Ro7McrLT8WTDRQcsn7JuV/CCE/l9yeaOapxm21oa5U6HowL7Xj1/LKfNGZWT5b+XkwE
OAheP0v2GXi820qCGskfymz3lilvp3ZKMWvCq4EzYhwV0AJFp/s3OCprC8M2mrcdaphid+PU
A5bZlnviOayVZNeSO08DhGQs1ZkNfPYbonfECfyspHLJ6Kw3cGJ4h8Swp7olpH9j/p6QFPviuF
yC9gOQlWdJ0LCMamQnkRjtqA91aBusX4bXx4d6uZoo7iZxhwAjhcHSKftzH1JHZK6YvX3f7T
UYPw0L0/UAM7XoMh4grGKz3E6qsCuG45mn1gJE3NUoEPSxGvXBOOEczH1sWH5wZt65Qd
UdFOUzzBT6iGDUYpamol+QNIuCbW9mu5qJ/gzNI1ueKYSfFPJQcXZUFFsiAzjurXbNAvc/BRk
FIEFAcwwleoHAQcuBP4w004DFiC53SVwRRhK5v6U4le1YwPYsg1uufeAPDtON95y+3Y/7tc
5Pi9Fi553241hm+LQb1dtAFTKfLLJY28aDLyCrKtdcZAzh4II2EAptf85arz7ueEYT+6lzm44HZtu
x5+tm1jsGSxwonpKTYyBcgdzwnsnJ6vrlxUPUNTsjOFdIOl4Qqpjzd60/3K0ff5wku12lNplzbU
UciBN44QrbEH3S7kvrjyeJzP5PtlMgoN5tJzxsZ4o3ZyK3m8iVICsj6MTRbN6OOjt8Y5pD4z4w
M6oaD5PDh6dHIY+cDJE6/XY4SO4kcf3joqkTtwEKJt+m3nZ3Uu0aGCTsj2EYvOqKi1TbI208X
NQ/bOBiDR4aWILjG/aHH6rhkgaWekO7QuzH03rC6Fc5zndAuJhDIKLUPkziU8k4YxpXgCmH
Mk8cgJpSwNj6pZe/JkLV1C6NVph5n6WVqPBlNj084fbbEk80f4lm13R8QaqbMwu8hpd8oVc
q3nt0LJwrzQZ06WZfgVLs1BgTs5nrN3M5bZ71Q55qRqO1cuHaCbJz9GxfkEXvNsFHeJecUZ0
DLAWDDI6TlIrtvQQqu3S2Pfr6lw/vOjzygfdesPzSHMr3RJEJxr1K9Sws/f1kH5VEcdO22JmW
L93JC07OKXbsuVDnQwCaxbi2JtPYSVlu6WWhoNUXaEaaaOH3QyK3ZKYQ9U53JlZOwYK1z/dE
sUrlZm5w/3urNVJyTNaBUkwguroCr0qVzZIHcT650lja9UB6BJyiDAzFSNuY93ZnRPJzNLnlcL8L
XP+382Oc3FfbxfX5Bfa4mj0uh/frxNdL4z8BGgy4ig==">
<INPUT TYPE="hidden" NAME="MD" VALUE="echo">

<INPUT TYPE="submit" value="Submit">

```

Where:

**merchant-return-URL** is the merchant site URL where to receive the authentication result from VISA.

**PaRes** is Payment authentication response which is returned by VISA directory.

**MD** is the value which the merchant has set when he submitted the authentication request (STEP 3).

#### Step 5:

There are six steps the merchant must complete:

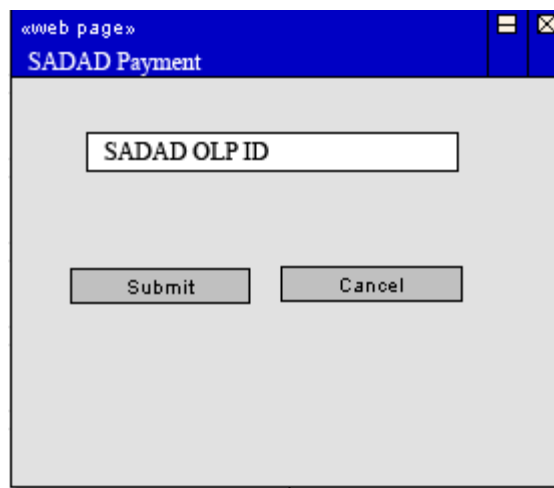
- A- The merchant gets the form content of **PaRes** and add it to the new request (mentioned in point A) associated with a parameter name "PARes".
- B- The merchant should generate a new secure hash for the new request, including the newly added parameters.
- C- Before sending the request, "PARes" parameters should be UTF-8 URL encoded.
- D- Then the merchant can submit the request to SmartRoute using **API Approve** in order to complete the payment cycle.

## 4.5. Appendix E: SADAD Implementation

If the “PaymentMethod” was “2” and the “Response.StatusCode” in an **API Payment** or **API mPayment** was returned as 20002 then the merchant must proceed with SADAD implementation as follows:

### Step 1:

Shopper browses at merchant site, adds items to shopping cart, then finalizes purchase. Merchant now has all necessary data, including SADAD OLP ID

A screenshot of a web browser window. The title bar says «web page». The page has a blue header with the text «SADAD Payment». Below the header is a light gray form area. Inside the form, there is a text input field with the placeholder text «SADAD OLP ID». Below the input field are two buttons: «Submit» and «Cancel».

### Step 2:

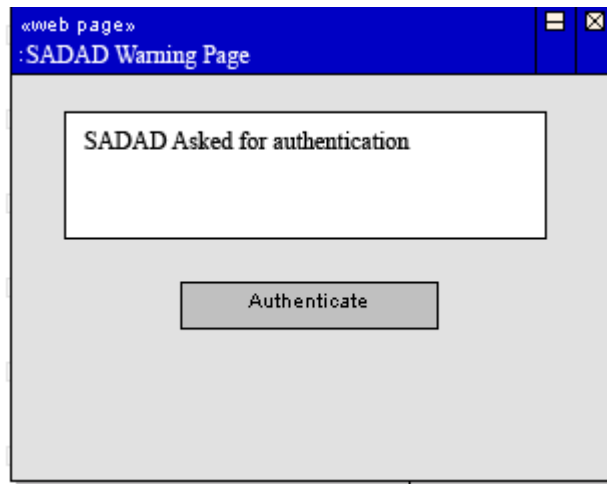
The merchant sends the information to SmartRoute using API Payment or API mPayment, which in turn initiates a call to SADAD to retrieve the following parameters which are returned to the merchant:

- Response.ESTN
- Response.MFU
- Response.AuthenticationURL

The merchant will use “Response.AuthenticationURL” to popup or redirect the user to the SADAD URL (Response.AuthenticationURL) where the customer must authenticate his/her payment request. Also, the merchant receives additional fields “Response.estn” which is the ENCRYPTED SADAD TRANSACTION NUMBER received from SADAD and “Response.mfu” which the merchant has already sent SmartRoute using the parameter “mfu” which represents the landing page which issuer will redirect to once the authentication is done.

### Step 3:

The merchant then constructs a page requesting the user to authenticate his payment request.



The following are mandatory fields which must be contained in the form (Authenticate)

```
<form name="AutoSubmitForm" action="<%= Response.AuthenticationURL %>"
method="GET">
<input type="hidden" name="mfu" value="<%=Response.mfu%>">
<input type="hidden" name="estn" value="<%= Response.estn%>">
<INPUT name="submit" value="Authenticate" type="submit" >
</form>
```

Where:

**Response.AuthenticationURL:** is returned by SmartRoute

**Response.estn** is returned by SmartRoute

**Response.mfu** is returned by SmartRoute

#### Step 4:

An authentication screen will be displayed where the user is asked to enter his SADAD Account Password as the following:

### Step 5:

The user will have to authenticate the payment as shown in the below picture:

Transaction Details

Merchant Name:

Payment Amount:52.81

Payment Currency:SAR

Date:03/03/2017

SADAD Account Balance:


SADAD Transaction ID:

Transaction Reference Number:0000035019


Second Level Authentication

Select Your Secret Image \*:


☐




☐




☐




☐




☐




☐



☐



☐



Select A One Time Password Method \*:

☐ SMS

☐ ANB Tawtheeq

### Step 6:

SADAD will now redirect the customer to the merchant using the **mfu** parameter passed in step 3. The response will include the parameter “**estn**” which shall be sent back to SmartRoute when initiating the API Approve request.

Note: the “**estn**” parameter in API Payment or API mPayment received from SmartRoute is different than the one received from issuer side and the later one should be used in API Approve.