e-Dirham G2 Payment Gateway

وزارة المالية
Ministry of Finance

NBAD

Payment Router-Integration Document

Version 1.4

sts

Document Control

History

Name	Version	Date (Day Month, YYYY)	Changes	Status
STS PN	1.0	10 August, 2014		Published
STS PN	1.01	25 January, 2015	Add Sample code for the redirect payment request and auto-update request.	
STS PN	1.1	5 January, 2015	Added support for Dynamic fees on eService Inquiry	
STS PN	1.2	17 February, 2015	Added support for eDirect & eDebit messages	
STS PN	1.3	19th April, 2015	Added recommendation for storing secret key Changing the secure-hash algorithm to HMAC-SHA256	
STS PN	1.4	28th April, 2015	Updates on Secret Key Configuration	
		20th May, 2015	Updates on Sample code used to send the payment request	

Distribution List

Name	Role	Comments

Table of Contents

INTRODUCTION

This document is intended for merchant system designer and developer planning to integrate with e-Dirham Payment Router interface to perform e-Commerce through e-Dirham system. Readers of this document should meet the requirements below:

- Experience in web application development.
- Have a background in payments services.

Purpose

This guide is written for merchants who have signed up through e-Dirham system to use it as their e-Payment processor and e-Dirham Payment Router Interface as their integration point for handling electronic transactions (payment, refund, auto update.. etc.) and from different payment methods (credit card, accounts…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.

Scope

This guide describes e-Dirham Payment Router programming interfaces details, along with guidelines and best practices for presenting these payment offerings.

Definitions, Acronyms and Appreviations

- PR : Payment Router

Pre-Request

- Merchant has signed an agreement with e-Dirham System.
- Merchant is provided with an e-Dirham System profile to generate unique Secret Key used for integration.

Overview

In order to fully document all the aspects of the API, this document contains the following:

- The integration
- Merchant Data Integrity And authentication
- Supported Transactions

THE INTEGRATION

Merchants interact with e-Dirham System to perform the tasks needed to execute electronic transactions through a secure channel.
The Merchant site will:

- Construct and submit a request consisting of pre-defined parameters with payment information collected by merchant site in the required format to integrate with e-Dirham System.

- Parse the response received from e-Dirham System containing transaction status.

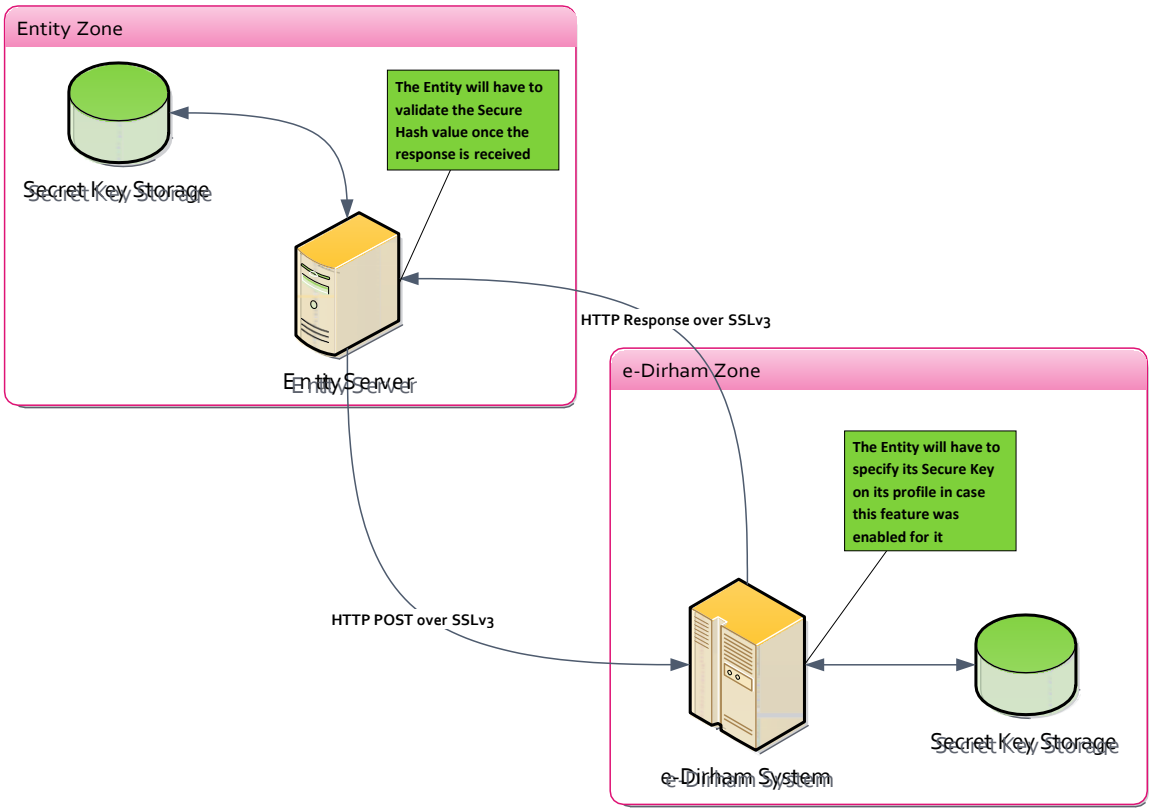

Figure 1: Shows the high level relationship between merchant site and e-Dirham System

MERCHANT DATA INTEGRITY AND AUTHENTICATION

Data Integrity

To Guarantee request/response data integrity a Secure Hash will be generated for each message, this Secure Hash will be created using critical message fields i.e. transaction amount. 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 a Secret Key will generated/set, this Merchant Secret Key is used as part of the Secure Hash value, and as a key to the secure-hash algorithm, Secret Key will only be known to Merchant application and e-Dirham system accordingly when message receiver (Merchant or e-Dirham system) will include Secret Key value when generating the Secure Hash value.

Setting Secret Key

PR- Merchant logs into e-Dirham Merchant Web management console to generate/set the Secret Key check Appendix E: Merchant Admin - Secret Key Configuration to configure the Secret Key, the generated Key will be stored securely at e-Dirham system side and Merchant copies this value and securely store it into his application to later use it during communication with e-Dirham system, this value is only known to the Merchant as it is stored encrypted at e-Dirham system. Check *Appendex F*: Security recommendations in handling the secret key

Request Flow

- Merchant prepares request message
- Merchant generates Secure Hash using request parameters and Secret Key value
- Merchant sends request and Secure Hash to e-Dirham System
- e-Dirham System upon receiving the request will retrieve Secret Key value stored for this merchant at e-Dirham system
- e-Dirham System regenerates Secure Hash using received request parameters and merchant Secret Key stored at e-Dirham System.
- e-Dirham System compare generated Secure Hash with received Secure Hash, if values mismatch request will be rejected. Else e-Dirham will continue processing request.

Response Flow

- e-Dirham System prepares response for merchant request
- e-Dirham System generate Secure Hash using response parameters and Merchant Secret Key stored at e-Dirham System
- e-Dirham System sends response and Secure Hash to Merchant

- Merchant upon receiving the response will use response parameter and Secret Key value stored at Merchant application to regenerate Secure Hash for response
- Merchant compare generated Secure Hash with received Secure Hash, if values mismatch response will be rejected. Else Merchant application will continue processing response

Merchant must make sure to:

- Store the Secret Key in a secure place as a secure database or file.
- Change the Secret Key periodically according to the Merchant Organization's Security policies.
- Not store the Secret Key within the source code of an ASP, JSP or any web page standing the chance of being accessed or viewed via web.

SUPPORTED TRANSACTIONS

Merchants can use the Payment Router to perform the following transactions:

- e-Service Inquiry Transaction
- Redirect Payment Transaction
- Redirect Pre-Authorization (Capture Transaction)
- Completion of Pre-Authorization Transaction
- Refund Transaction
- Void Transaction
- Transaction Confirmation (Auto Update)
- Reversal Transaction
- Inquiry Status Transaction
- Redirect e-Debit Pay
- Back-to-Back e-Debit Status Delivery

- Back-to-Back e-Debit Status Update

Comunication With edirham

Before using the Payment Router interface, the integrator should understand the Payment Router Post integration page and its parameters, as well as their effects on the integration process.
Sending and receiving transactions between Payment Router System and Merchant site is done using a redirect model.

- **Redirection communication model:** in this model a merchant site will redirect a customer (card holder) browser to Payment Router system payment site where the customer is requested to provide input to complete the cycle.

- **Back to back communication model**: where Merchant site sends request to e-Dirham Payment Router back-to-back URL using HTTP POST and waits for a response from e-Dirham System. Back to back communication with e-Dirham system is transparent from customer (card holder) point of view, the customer (card holder) can and will only view Merchant site pages.

MESSAGE STRUCTURE RULE

Message syntax is:

- Data is in name/value pairs.
- Names are case sensitive.
- All the messages must be encoded using UTF-8 charset.

E-SERVICE INQUIRY ACTION

For this type of transaction merchant web application handle the communication with e-Dirham System using Back-to-Back Model please refer to section *Communication with EDirham*.

Detailed Integration Process

This section describes the main items merchant integrator needs to know, to prepare and send an e-Service Inquiry request before the actual payment or Pre-Authorization transaction.

Request

The below tables describes the parameters for the e-Service Inquiry action, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Mandatory Parameters		
Action	2	Alphanumeric value representing the action to be called 28 for eService inquiry.
BankID	10	Alphanumeric value representing e-Dirham System ID, this value is provided by e-Dirham System operation team upon merchant enrollment.
MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
TerminalID	8	Alphanumeric value provided by e-Dirham System operation team upon merchant enrollment.
ApplicationNumber	20	Alphanumeric value provided by the merchant.
TransactionRequestDate	14	Alphanumeric value representing the request date time stamp formatted as the following (ddMMyyyyHHmmss).
SecureHash	64	Alphanumeric value representing generated hex-encoded hash using hashing algorithm HMAC-SHA256, by concatenating parameters as a single string starting with the merchant's secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character, null values are not passed to the secure hash, the secret key will be also the key to be passed to the algorithm. The Parameters to use: secretKey Action ApplicationNumber BankId Currency MainCodeSubCode Quantity Price ExtraFields_intendedEDirhamService MerchantId PaymentMethodType TerminalId

		TransactionRequestDate(ddMMyyyyHHmmss) UniqueTransactionId Version Example: bankId =MOFPG420 terminalId =123 applicationNumber =123 transactionRequestDate =31082014163243 uniqueTransactionId =1409491949239 currency =784 paymentMethodType =1-1 extraFields_intendedEDirhamService =0 version =null action =28 merchantId =edConnectM Secret Key: 76a0ed27b643bc6652273f29df66e522 The input to the Secure Hash generation routine would be: **76a0ed27b643bc6652273f29df66e52228123MOFPG4207840edConnectM1-1123310820141632431409491949239** Output: **bqQv7SMPlIJ9+q2JV53uWIaCt2k5iV4QN+XROREeRoM=**
UniqueTransactionID	20	The unique number of the payment order (transaction) generated by the Merchant, it represent a unique identifier for the transaction, and it is alphanumeric.
Currency	3	The numeric ISO Code for the currency and not the character value, e.g.: 840 for US Dollar
PaymentMethodType	3	A value representing the payment method type used by the user based on the card: 1-11: Visa Card 1-22: Master Card 1-99: GII Co-branded Mag-Stripe Card 1-10Personal GII Co-Branded Chip Card 1-11: Corporate GII Co-Branded Chip Card

		1-12: GII PLC Mag-Stripe Card 1-13: GII PLC Chip Card
ExtraFields_intendedEDirhamService	2	The intended e-Dirham Service that is going to be executed after the e-Service inquiry. Expected values: 0: Pay web 32: Pre-Authorize web
e-Service Details parameters, Mandatory		
The e-Service inquiry request can handle multiple eservices in one request, and for all the details of an e-Service the parameter should be concatenated with a number starting with one for service 1 and 2 for service 2 … etc. **Ex: Sending a request with two e-Services with information as the following:** **e-Service 1: Code=000000-0001, Price=10, Quantity=2** **e-Service 2: Code=000000-0002, Quantity=4** **The request parameters should be added as the following:** **EServiceMainCodeSubCode_1 = 000000-0001, EServiceQuantity_1 = 2, EServicePrice_1 =10** **EServiceMainCodeSubCode_2 = 000000-0002, EServiceQuantity_2 =4**		
EServiceMainCodeSubCode_*	12	An alphanumeric value representing the e-Service MainCode-SubCode as XXXXXX-XXXX * Should be replaced with a number for each e-Service group
EServicePrice_*	12	A numeric value representing the price of an eService, this parameter is used only for a ZERO amount e-Service. The value should be ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100 * Should be replaced with a number for each e-Service group
EServiceQuantity_*	6	A numeric value representing the quantity required for each eService. * Should be replaced with a number for each e-Service group
Optional Parameters		

Version	1	Alphanumeric value representing the version of the action to execute (1.0 is the default).

Response

- After executing the request a response from e-Dirham System will be returned with Status code, please refer to *Appendix B* - *E-Service inquiry Response Codes* for Status Codes.
- Verify the received secure hash based on the received parameters described in the table 2.
- Verify the success of execution by checking the Status code from the received parameter.
- Apply the required business logic based on the transaction result.

The below tables describes all the response parameters returned by e-Dirham System in the response stream, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Response.Status	30	Alphanumeric value representing response code of the request. Please refer to section 5.2 for more details about the response codes values, descriptions and actions to take accordingly.
Response.StatusMessage	512	A string representing a message describing the response status as received from e-Dirham System.
Response.MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
Response.BankID	10	Alphanumeric value representing e-Dirham System ID, this value is provided by e-Dirham System operation team upon merchant enrollment.
Response.RetrievalRefNumber	15	Alphanumeric value representing a confirmation id generated by e-Dirham System as confirmation reference for the current payment transaction.
Response.UniqueTransactionID	20	The unique number of the payment order (transaction) generated by the Merchant, it represent a unique identifier for the transaction, and it is alphanumeric. (returned as in request)
Response.Currency	3	The numeric ISO Code for the currency and not the character value, e.g.: 840 for US Dollar
Response.PaymentMethodType	3	A value representing the payment method type used by the user based on the card: 1-11: Visa Card 1-22: Master Card 1-99: GII Co-branded Mag-Stripe Card 1-10Personal GII Co-Branded Chip Card 1-11: Corporate GII Co-Branded Chip Card 1-12: GII PLC Mag-Stripe Card 1-13: GII PLC Chip Card
Response.TerminalID	8	Alphanumeric value provided by e-Dirham System operation team upon merchant enrollment.
Response.EDirhamFees	30	An ISO formatted amount containing e-Dirham fees
Response.CollectionCenterFees	30	An ISO formatted amount containing the Collection Center fees.
Response.TransactionAmount	12	An ISO formatted amount containing the total transaction amount (amount to be paid).
Response.SecureHash	64	Alphanumeric value representing generated hex-encoded hash using hashing algorithm HMAC-SHA256, by

concatenating parameters as a single string starting with the merchant's secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character, null values are not passed to the secure hash, the secret key will be also the key to be passed to the algorithm.

The Parameters to use:
Response.SecretKey
Response.BankId
Response.CollectionCenterFees
Response.Currency
Response.EdirhamFees
Response.Amount
Response.TotalAmount
Response.Fees
Response.MainCodeSubCode
Response.EnglishDescription
Response.MinistryEnglishName
Response.MerchantId
Response.PaymentMethodType
Response.RetrievalRefNumber
Response.Status
Response.StatusMessage
Response.TerminalId
Response.TransactionAmount
Response.TransactionResponseDate(ddMMyyyyHHmmss)
Response.UniqueTransactionId
Example:
bankId = MOFPG420
retrievalRefNumber = 140000019854
uniqueTransactionId = 1409639442699
currency = 784
paymentMethodType = 1-1
terminalId = 123

		edirhamFees = 600 collectionCenterFees = 200 transactionAmount = 2300 transactionResponseDate = 02092014091922 price = null quantity = null mainCodeSubCode = 000000-0002 amount = 1000 totalAmount = 1500 fees = 500 MainCodeSubCode = null englishDescription = e-Serv 1ServServServServServServServServ arabicDescription = ???? 11???? 1???? 1???? 1???? 1???? 1??? ministryEnglishName = Ministry of Finance ministryArabicName = ???? 11???? 1???? 1???? 1???? 1???? 1??? status = 0000 statusMessage = Transaction was processed successfully. **secureHash =** 6Ve2TThkUDdt35FtabRletlsL3vTNoz7aqy8GS9Ob1s= merchantId = edConnectM The input to the Secure Hash generation routine would be: **76a0ed27b643bc6652273f29df66e522MOFPG4202007 8460010001500500e-Serv 1ServServServServServServServServMinistry of FinanceedConnectM1- 11400000198540000Transaction was processed successfully.123230002092014091922140963944 2699** Output: 6Ve2TThkUDdt35FtabRletlsL3vTNoz7aqy8GS9Ob1s=
Response.TransactionResponse Date	14	Alphanumeric value representing the response date using the following format: ddMMyyyyHHmmss Note: check Appendix A for descriptive details about the

		date format.
EServiceAmount_*	12	An ISO formatted amount containing the eService (price * quantity).
EServiceTotalAmount_*	12	An ISO formatted amount containing the e-Service (price * quantity) + e-Service owner fees.
EServiceFee_*	12	An ISO formatted amount containing the eService owner fees.
EServiceMainCodeSubCode_*	20	An alphanumeric value representing the e-Service MainCode-SubCode as XXXXXX-XXXX
EServiceEnglishDescription_*	40	An alpha numeric value representing the eservice English description configured on e-Dirham System.
EServiceArabicDescription_*	40	An alpha numeric value representing the eservice Arabic description configured on e-Dirham System.
EServiceMinistryEnglishName_*	40	An alpha numeric value representing the eservice Owner English name configured on e-Dirham System.
EServiceMinistryArabicName_*	40	An alpha numeric value representing the eservice Owner Arabic name configured on e-Dirham System.
Response.ResponseDynamicFeesDetails	Represents a JSON array that contains details for Dynamic Fees, object fields and example are shown below.	
amount	12	An ISO formatted amount containing the current fee amount.
englishDescribtion	30	The English description of the Dynamic fee.
arabicDescribtion	30	The Arabic description of the Dynamic fee.
Order	1	The order of the current Dynamic fee.
operation	1	Empty value.

Sample:

Response.ResponseDynamicFeesDetails=


```
[
 {
  "amount":"200",
  "englishDescribtion":"fee1",
  "arabicDescribtion":"قلومع1",
  "order":"0",
  "operation":null
 },
 {
  "amount":"300",
  "englishDescribtion":"fee2",
  "arabicDescribtion":"قلومع 2",
  "order":"1",
  "operation":null
 }
]
```

PAYMENT (PAY-WEB) ACTION

For this type of transaction merchant web application handle the communication with e-Dirham System using Redirect Model please refer to section *Communication with EDirham*.
This section describes the main items merchant integrator needs to know, for building pages integrating merchant web application with e-Dirham System through Payment Router in order to perform payment transactions.

Request

- Collect the payment information from the customer with the information of the Inquired e-Service/s or provide extra details if no eservice inquiry is performed.
- Submit the request to e-Dirham System using Redirect HTTP POST using the provided Redirect Link.

The below tables describes all the request parameters that must be collected by merchant site and provided to the PMR POST redirect link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Mandatory Parameters		
Action	2	Alphanumeric value representing the action to be called 0 for Pay Web.
BankID	10	Alphanumeric value representing e-Dirham System ID, this value is provided by e-Dirham System operation team upon merchant enrollment.
MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
Currency	3	The numeric ISO Code for the currency and not the character value, e.g.: 840 for US Dollar
PUN	20	The unique number of the payment order (transaction) generated by the Merchant, it represent a unique identifier for the transaction, and it is alphanumeric.
PaymentDescription	255	Alphanumeric string containing a narrative description of the payment order using the language specified in the language parameter. This value should be HTML encoded.
MerchantModuleSessionID	256	Alphanumeric value representing the merchant web session id initiating the payment request.
TransactionRequestDate	14	Alphanumeric value representing the request date time stamp formatted as the following (ddMMyyyyHHmmss).
SecureHash	64	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 secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character. The Parameters to use: **secretKey** **Action** **BankId** **Currency** **Amount** **ExtraFields_f17** **ExtraFields_f16** **ExtraFields_f18** **Lang**

MerchantId

MerchantModuleSessionId

NationalId

PaymentDescription

Pun

TransactionRequestDate

Version

Example:

MerchantID =edConnectM

Action =0

Lang =en

BankID =MOFPG420

Currency =784

MerchantModuleSessionID =jIHDpGpgP7O3pvvtHgrj_kt

PaymentDescription =PaymentRouter+Sample+Payment

ExtraFields_f18 =123

ExtraFields_f17 =1409491949239

ExtraFields_f16 =1-1

PUN =1409492646898

NationalID =8897871212

Amount =2300

TransactionRequestDate =31082014165104

Secret Key: 76a0ed27b643bc6652273f29df66e522

The input to the Secure Hash generation routine would be:

76a0ed27b643bc6652273f29df66e5220MOFPG4207842 30014094919492391- 1123enedConnectMjIHDpGpgP7O3pvvtHgrj_kt889787 1212PaymentRouter Sample Payment14094926468983108201416510 4null

Output:

c919e69c50ee6a993ced79683e250a673375ab450078a 496117170e203f1df1a

OR

secretKey

Action
BankId
Currency
ApplicationNumber
ExtraFields_intendedEDirhamService
MainCodeSubCode
Quantity
Price
ExtraFields_f16
ExtraFields_f18
Lang
MerchantId
MerchantModuleSessionId
NationalId
PaymentDescription
Pun
TransactionRequestDate
Version

Example:
MerchantID = edConnectM
Action = 0
ExtraFields_intendedEDirhamService = 0
Lang = en
BankID = MOFPG420
Currency = 784
EServiceMainCodeSubCode_1 = 000000-0002
MerchantModuleSessionID = jlHDpGpgP7O3pvvtHgrj_kt
PaymentDescription = PaymentRouter+Sample+Payment
ExtraFields_f18 = 123
ExtraFields_f16 = 1-1
PUN = 1409493438621
EServiceQuantity_1 = 1
NationalID = 8897871212
ApplicationNumber = 123

		TransactionRequestDate = 31082014165812 Secret Key: 76a0ed27b643bc6652273f29df66e522 The input to the Secure Hash generation routine would be: **76a0ed27b643bc6652273f29df66e5220123MOFPG4207 8414094934386211- 1123enedConnectMjIHDpGpgP7O3pvvtHgrj_kt889787 12121409493438621PaymentRouter+Sample+Payment 31082014165812** Output: **JCvE/lACmY+AyPvHMabN+OudKM5hMGkOVUu467iAR5U=**
ExtraFields_f16	3	Payment method type: 1-1: Visa Card 1-2: Master Card 1-99: GII Co-branded Mag-Stripe Card 1-10Personal GII Co-Branded Chip Card 1- 11: Corporate GII Co-Branded Chip Card 1-12: GII PLC Mag-Stripe Card 1-13: GII PLC Chip Card
ExtraFields_f18	8	The Terminal Id that was assigned to the merchant during the enrollment process for use with e-commerce transactions.
Optional parameters		
ExtraFields_f14	512	Merchant site response page URL that will receive the response from e-Dirham System, this can help merchant having different response pages based on the requested service or any other criteria.
NationalID	32	Alphanumeric value representing the national id of the customer performing the transaction. If this field is not required to be filled by e-Dirham System, it can be set to Empty String: “”. Please consult e-Dirham System operation team for more information.
Lang	2	Alphabetic value representing the language of the interface displayed to customer at merchant site, and used as language for the payment description parameter. e-Dirham System will use this value to display the interface supporting selected language to the customer during the payment process. Supported values are: En Ar
Conditional Parameters		
Option 1		

ExtraFields_f17	20	E-Service inquiry unique transaction Id.
Amount	12	A numeric value containing the total transaction amount ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100
Option 2		
ApplicationNumber	20	Alphanumeric value provided by the merchant.
ExtraFields_intendedEDirhamService	2	The intended e-Dirham Service that is going to be executed after the e-Service inquiry. Expected values: 0: Pay web 32: Pre-Authorize web
e-Service Details parameters, Mandatory		
The e-Service inquiry request can handle multiple eservices in one request, and for all the details of an e-Service the parameter should be concatenated with a number starting with one for service 1 and 2 for service 2 … etc. **Ex: Sending a request with two e-Services with information as the following:** **e-Service 1: Code=000000-0001, Price=10, Quantity=2** **e-Service 2: Code=000000-0002, Quantity=4** **The request parameters should be added as the following:** **EServiceMainCodeSubCode_1 = 000000-0001, EServiceQuantity_1 = 2, EServicePrice_1 =10** **EServiceMainCodeSubCode_2 = 000000-0002, EServiceQuantity_2 =4**		
EServiceMainCodeSubCode_*	12	An alphanumeric value representing the e-Service MainCode-SubCode as XXXXXX-XXXX * Should be replaced with a number for each e-Service group
EServicePrice_*	12	A numeric value representing the price of an eService, this parameter is used only for a ZERO amount e-Service. The value should be ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100 * Should be replaced with a number for each e-Service group
EServiceQuantity_*	6	A numeric value representing the quantity required for each eService.

		* Should be replaced with a number for each e-Service group
Optional Parameters		
Version	1	Alphanumeric value representing the version of the action to execute (1.0 is the default).

Response

The below tables describes the parameters for the Pay Web action, all the parameters are case sensitive without whitespaces

- Merchant site response page receives the response from e-Dirham System.
- Verify the received secure hash based on the received parameters.
- Verify the success of execution by checking the response code from the received parameter.
- Apply the required business logic based on the transaction result.

The below tables describes all the response parameters posted back from e-Dirham System, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Response.Status	30	Alphanumeric value representing the response code, this code covers both errors generated PMR interface e-Dirham System. Please refer to section 5.2 for more details about the response codes values, descriptions and actions to take accordingly.
Response.ConfirmationID	15	Alphanumeric value representing a confirmation id generated by e-Dirham System as confirmation reference for the current payment transaction
Response.StatusMessage	512	Alphanumeric value representing a message describing the response status as received from e-Dirham System using the language specified in the request; this parameter will be filled only after a complete execution process. This parameter encoding is UTF-8 for all languages
Response.TransactionResponseDate	14	Alphanumeric value representing the response date using the following format: ddMMyyyyHHmmss Note: check Appendix A for descriptive details about the date format.
Response.SecureHash	64	Alphanumeric value representing generated hex-encoded hash using hashing algorithm HMAC-SHA256, by concatenating parameters as a single string starting with the merchant's secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character, null values are not passed to the secure hash, the secret key will be also the key to be passed to the algorithm. The Parameters to use: secretKey Response.Amount Response.BankID Response.CollectionCenterFees Response.ConfirmationID Response.Currency Response.EDirhamFees Response.EServiceData merchantId Response.MerchantModuleSessionID Response.RES_PAYMENT_METHOD_TYPE Response.PUN

		Response.Status Response.StatusMessage 76a0ed27b643bc6652273f29df66e5222300MOFPG4202001 0002'],'price':['1000'],'amountWithFees':[1000],'quantity':[' 114109611962810000Transaction+was+processed+successf Response.TransactionResponseDate Response.TerminalID Example: The input to the Secure Hash generation routine would be: Output: **0098f748ed429cbcc5d00363ab0c862fee622744785270d1 1df833e3fac3145d**
Response.Amount	12	A numeric value containing the total transaction amount ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100
Response.Currency	**3**	The numeric ISO Code for the currency and not the character value, e.g.: 840 for US Dollar
Response.MerchantModuleSessionID	**256**	Alphanumeric value representing the merchant web session id initiating the payment request.
Response.PUN	**20**	The unique number of the payment order (transaction) generated by the Merchant, it represent a unique identifier for the transaction, and it is alphanumeric.
Response.BankID	**10**	Alphanumeric value representing e-Dirham System ID, this value is provided by e-Dirham System operation team upon merchant enrollment.
Response.TerminalID	**8**	The Terminal Id that was assigned to the merchant during the enrollment process to use it with e-commerce transactions.
Response.ReceiptID	**15**	Alphanumeric value representing a receipt id generated by eD-Wallet System as receipt reference for the current payment transaction
Response.CollectionCenterFees	**12**	A numeric value containing a collection center fees ISO Formatted with no decimal point, e.g.: 1.00 AED sent as 100
Response.EDirhamFees	**12**	A numeric value containing an eDirham fees ISO Formatted with no decimal point, e.g.: 1.00 AED sent as 100
Response.TransactionAmount	**12**	A numeric value containing the total transaction amount ISO Formatted with no decimal point,

		e.g.: 1.00 AED sent as 100
Response.EServiceData		
mainSubCode	12	An alphanumeric value representing the e-Service MainCode-SubCode as XXXXXX-XXXX Ex: 000000-0001
Price	12	A numeric value representing the price of an eService, this parameter is used only for a ZERO amount e-Service. The value should be sent normaly as the Price value as 22.55 AED
quantity	6	A numeric value representing the quantity for each eService.
ownerFees	12	A numeric value containing an owner fees ISO Formatted with no decimal point, e.g.: 1.00 AED sent as 100
amountWithoutFees	12	A numeric value containing the total amount for a specific service (price*quantity) exclude the owner fees The amount must be formatted as ISO Formatt with no decimal point, e.g.: 1.00 AED sent as 100
amountWithFees	12	A numeric value containing the total amount for a specific service (price*quantity+ownerFees) include the owner fees The amount must be formatted as ISO Formatt with no decimal point, e.g.: 1.00 AED sent as 100

All payment request parameters passed as simple parameters except the eService details(if exist), it must be passed as JSON array object as follow:

EServiceData:

```
[
   {
      "mainSubCode": "000000-0005",
      "price": "",
      "quantity": "1"
   },
   {
      "mainSubCode": "000000-0001",
      "price": "",
      "quantity": "1"
   },
   {
      "mainSubCode": "000000-0002",
      "price": "22.25",
      "quantity": "1"
   }
]
```

Figure 2 EServiceData Parameter sample

Sample Code For Sending The Request

The below code sample shows how a merchant can send redirect payment request to the PMR:

```
public void doRedirectPayment(HttpServletRequest req,
            HttpServletResponse response) throws Exception {

        try {
            // Hash Parameters
            String parametersToHash = getParamteresToHash();
            String secretKey = "[Value of Merchant Secret Key]";
            String secureHash =
generateHMACSHA256Hash(parametersToHash,secretKey);

            req.setAttribute("TransactionRequestDate", "22012015135919");
            req.setAttribute("Amount", "300");
            req.setAttribute("PaymentDescription",
                  URLEncoder.encode("Sample Description", "UTF-8"));
            req.setAttribute("NationalID", "[Value of National ID]");
            req.setAttribute("PUN", "1414414845606");
            req.setAttribute("MerchantModuleSessionID",
                  "KaWLRu2mHEVjfSATzcxJNoy");
            req.setAttribute("MerchantID", "[Value of Merchant ID]");
```

```
            req.setAttribute("BankID", "[Value of Bank ID]");
            req.setAttribute("Lang", "en");
            req.setAttribute("RedirectURL", "http://www.website.com"
                  + "/PaymentRouter/AcceptRedirectRequestServlet");
            req.setAttribute("Action", "0");
            req.setAttribute("Currency", "784");
            req.setAttribute("ExtraFields_f14", "http://www.mywebsite.com"
                  + "/Simulator/RedirectPaymentRouterPaymentResponse.do");
                  // The URL that the response will be redirected to
            req.setAttribute("ExtraFields_f16", "1-1"); // Payment Method
            req.setAttribute("ExtraFields_f17",
                        "[Value of e-Service Inquiry PUN If Exists]");
            req.setAttribute("ExtraFields_f18", "[Value of Terminal ID]");

            // set the hash in the request
            req.setAttribute(PaymentRouterParameters.SECRET_HASH,
                        secureHash);

            // set the EService Inquiry Parameters
            // if no EserviceInquiryId exist
            if("[Value of e-Service Inquiry PUN If Exists]" == null ||
                  "[Value of e-Service Inquiry PUN If Exists]".equals("")) {
                  // This if statement doesn't make sense syntax wise, it's
                  // just to show that this block is reached only
                  // if the e-Service Inquiry PUN doesn't exist
                req.setAttribute("ApplicationNumber", "123");
                req.setAttribute("EServiceMainCodeSubCode_1",
                        "000000-0001");
                req.setAttribute("EServiceQuantity_1", "1");
                req.setAttribute("EServicePrice_1", "100");
                req.setAttribute("intendedEDirhamService", "0");
            }

            // The JSP page that contains a form that will be submitted
            // to send the redirect request
            response.sendRedirect("sample.jsp");
        } catch (Exception e) {
            e.printStackTrace();
        }
    }

    private String getParamteresToHash() {
        StringBuilder sb = new StringBuilder();
          sb.append("[Value of Merchant Secret Key]") // Secret Key
          .append("0") // Pay Action
          .append("[Value of Bank ID]") // Bank ID
          .append("784"); // Currency

          if("[Value of e-Service Inquiry PUN If Exists]" != null &&
            "[Value of e-Service Inquiry PUN If Exists]".length() > 0) {
```

```
            // This if statement doesn't make sense syntax wise, it's
            // just to show that this block is reached only
            // if the e-Service Inquiry PUN exists
            sb.append("300") // Amount
            .append("[Value of e-Service Inquiry PUN If Exists]");
            // ExtraFields_f17 : e-Service Inquiry PUN
          } else {
             if("000000-0001" != null && "000000-0001".length() > 0){
                   // This if statement doesn't make sense syntax wise,
                   // it's just to show that this block is reached only
                   // if the e-Service main and sub code exist
                   sb.append("123") // Application Number
                   .append("0") // Intended EDirham Service
                   .append("000000-0001")
                   // EServiceMainCodeSubCode_1 : The code of the eService
                     .append("1")
                     // EServiceQuantity_1 : The quantity of the eService
                     .append("100");
                   // EServicePrice_1 : The price of the e-Service
               }
          }

          sb.append("1-1") // Payment Method
          .append("[Value of Terminal ID]") // Terminal ID
          .append("en") // Language
          .append("[Value of Merchant ID]") // Merchant ID
          .append("KaWLRu2mHEVjfSATzcxJNoy") // Merchant Module Session ID
          .append("[Value of National ID]") // National ID
          .append("Sample Description") // Payment Description
          .append("1414414845606") // Payment Unique Number (PUN)
          .append("22012015135919") // Transaction Request Date


        return sb.toString();
    }
              String generateHMACSHA256Hash(String data, String
merchantSecretKey) {
        String result = "";

            {
            String HMAC_SHA256_ALGORITHM = "HmacSHA256";

            // Get an HMAC SHA256 key from the raw key bytes
            SecretKeySpec signingKey =
SecretKeySpec(merchantSecretKey.getBytes(), HMAC_SHA256_ALGORITHM);

            // Get an HMAC SHA256 Mac instance and initialize with the
signing key
            Mac mac = Mac.getInstance(HMAC_SHA256_ALGORITHM);
            mac.init(signingKey);
```

```
            // Compute the HMAC on input data bytes
                [] rawHmac = mac.doFinal(data.getBytes());

            // Convert to hexadecimal
            result = Hex.encodeHexString(rawHmac);

            // Base64-encode the HMAC
            result =     String(Base64.encodeBase64(result.getBytes()));
        }       (NoSuchAlgorithmException e) {
            e.printStackTrace();
        }       (InvalidKeyException e) {
            e.printStackTrace();
        }

                result;
    }
```

Please notice the comments in the code, especially for the if statements. The "sample.jsp" page contains a form that will read those parameters that are set in the request, and use the parameter set in the "RedirectURL" in the action attribute of the form. Then, the form should be submitted automatically using JavaScript, and thus the page will be redirected to the PMR.

PRE-AUTH (WEB) ACTION

For this type of transaction merchant web application handle the communication with e-Dirham System using Redirect Model please refer to section *Communication with EDirham*.
This section describes the main items merchant integrator needs to know, for building pages integrating merchant web application with e-Dirham System through PMR in order to perform Pre-Auth transactions.

Request

- Collect the payment information from the customer with the information of the Inquired e-Service/s.

- Submit the request to e-Dirham System using Redirect HTTP POST using the provided Redirect Link.

The below tables describes all the request parameters that must be collected by merchant site and provided to the Payment Router POST redirect link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Mandatory Parameters		
Action	2	Alphanumeric value representing the action to be called 0 for Pay Web.
BankID	10	Alphanumeric value representing e-Dirham System ID, this value is provided by e-Dirham System operation team upon merchant enrollment.
MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
Currency	3	The numeric ISO Code for the currency and not the character value, e.g.: 840 for US Dollar
Amount	12	A numeric value containing the total transaction amount ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100
PUN	20	The unique number of the payment order (transaction) generated by the Merchant, it represent a unique identifier for the transaction, and it is alphanumeric.
PaymentDescription	255	Alphanumeric string containing a narrative description of the payment order using the language specified in the language parameter. This value should be HTML encoded.
MerchantModuleSessionID	256	Alphanumeric value representing the merchant web session id initiating the payment request.
TransactionRequestDate	14	Alphanumeric value representing the request date time stamp formatted as the following (ddMMyyyyHHmmss).
SecureHash	64	Alphanumeric value representing generated hex-encoded hash using hashing algorithm HMAC-SHA256, by concatenating parameters as a single string starting with the merchant's secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character, null values are not passed to the secure hash, the secret key will be also the key to be passed to the algorithm. The Parameters to use: **secretKey** **Action** **BankId** **Currency**

Amount
ExtraFields_f17
ExtraFields_f16ExtraFields_f18
Lang
MerchantId
MerchantModuleSessionId
NationalId
PaymentDescription
Pun
TransactionRequestDate
Version

Example:

MerchantID =edConnectM

Action =0

Lang =en

BankID =MOFPG420

Currency =784

MerchantModuleSessionID =jIHDpGpgP7O3pvvtHgrj_kt

PaymentDescription =PaymentRouter+Sample+Payment

ExtraFields_f18 =123

ExtraFields_f17 =1409491949239

ExtraFields_f16 =1-1

PUN =1409492646898

NationalID =8897871212

Amount =2300

TransactionRequestDate =31082014165104

Secret Key: 76a0ed27b643bc6652273f29df66e522

The input to the Secure Hash generation routine would be:

76a0ed27b643bc6652273f29df66e52202300123MOFPG4207841-1123enedConnectMjIHDpGpgP7O3pvvtHgrj_kt889787121214094934386 21PaymentRouter+Sample+Payment31082014165812

Output:

nL5gd2j/4YSHPzXLV11e2+yXGMQMZ+/0geHeVCFhwOg=

OR

secretKey
Action
BankId
Currency
ApplicationNumber
ExtraFields_intendedEDirhamService
MainCodeSubCode
Quantity
Price
ExtraFields_f16ExtraFields_f18
Lang
MerchantId
MerchantModuleSessionId
NationalId
PaymentDescription
Pun
TransactionRequestDate
Version

Example:
MerchantID = edConnectM
Action = 0
ExtraFields_intendedEDirhamService = 0
Lang = en
BankID = MOFPG420
Currency = 784
EServiceMainCodeSubCode_1 = 000000-0002
MerchantModuleSessionID = jlHDpGpgP7O3pvvtHgrj_kt
PaymentDescription = PaymentRouter+Sample+Payment
ExtraFields_f18 = 123
ExtraFields_f16 = 1-1
PUN = 1409493438621
EServiceQuantity_1 = 1

		NationalID = 8897871212 ApplicationNumber = 123 TransactionRequestDate = 31082014165812 Secret Key: 76a0ed27b643bc6652273f29df66e522 The input to the Secure Hash generation routine would be: **76a0ed27b643bc6652273f29df66e52202300123MOFPG420784000000-000214094934386211-11230enedConnectMjIHDpGpgP7O3pvvtHgrj_kt88978712121409493438621PaymentRouter+Sample+Payment31082014165812** Output: **a77L836Vc7EokMDf23vKmVePBcrXg9gOCMnkX2i2Im4=**
ExtraFields_f16	3	Payment method type: 1-1: Visa Card 1-2: Master Card 1-99: GII Co-branded Mag-Stripe Card 1-10Personal GII Co-Branded Chip Card 1-11: Corporate GII Co-Branded Chip Card 1-12: GII PLC Mag-Stripe Card 1-13: GII PLC Chip Card
ExtraFields_f18	8	The Terminal Id that was assigned to the merchant during the enrollment process for use with e-commerce transactions.
Optional parameters		
ExtraFields_f14	512	Merchant site response page URL that will receive the response from e-Dirham System, this can help merchant having different response pages based on the requested service or any other criteria.
NationalID	32	Alphanumeric value representing the national id of the customer performing the transaction. If this field is not required to be filled by e-Dirham System, it can be set to Empty String: “”. Please consult e-Dirham System operation team for more information.
Lang	2	Alphabetic value representing the language of the interface displayed to customer at merchant site, and used as language for the payment description parameter. e-Dirham System will use this value to display the interface supporting selected language to the customer during the payment process. Supported values are: En

		Ar
Conditional Parameters		
Option 1		
ExtraFields_f17	20	E-Service inquiry unique transaction Id.
Amount	12	A numeric value containing the total transaction amount ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100
Option 2		
ApplicationNumber	20	Alphanumeric value provided by the merchant.
ExtraFields_intendedEDirhamService	2	The intended e-Dirham Service that is going to be executed after the e-Service inquiry. Expected values: 0: Pay web 32: Pre-Authorize web
e-Service Details parameters, Mandatory		
The e-Service inquiry request can handle multiple eservices in one request, and for all the details of an e-Service the parameter should be concatenated with a number starting with one for service 1 and 2 for service 2 … etc. **Ex: Sending a request with two e-Services with information as the following:** **e-Service 1: Code=000000-0001, Price=10, Quantity=2** **e-Service 2: Code=000000-0002, Quantity=4** **The request parameters should be added as the following:** **EServiceMainCodeSubCode_1 = 000000-0001, EServiceQuantity_1 = 2, EServicePrice_1 =10** **EServiceMainCodeSubCode_2 = 000000-0002, EServiceQuantity_2 =4**		
EServiceMainCodeSubCode_*	12	An alphanumeric value representing the e-Service MainCode-SubCode as XXXXXX-XXXX * Should be replaced with a number for each e-Service group
EServicePrice_*	12	A numeric value representing the price of an eService, this parameter is used only for a ZERO amount e-Service. The value should be ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100 * Should be replaced with a number for each e-Service

		group
EServiceQuantity_*	6	A numeric value representing the quantity required for each eService. * Should be replaced with a number for each e-Service group
Optional Parameters		
Version	1	Alphanumeric value representing the version of the action to execute (1.0 is the default).

Response

- Merchant site response page receives the response from e-Dirham System
- Verify the received secure hash based on the received parameters.
- Verify the success of execution by checking the response code from the received parameter.
- Apply the required business logic based on the transaction result.

The below tables describes all the response parameters posted back from e-Dirham System, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Response.Status	30	Alphanumeric value representing the response code, this code covers both errors generated PMR interface e-Dirham System. Please refer to section 5.2 for more details about the response codes values, descriptions and actions to take accordingly.
Response.ConfirmationID	15	Alphanumeric value representing a confirmation id generated by e-Dirham System as confirmation reference for the current payment transaction
Response.StatusMessage	512	Alphanumeric value representing a message describing the response status as received from e-Dirham System using the language specified in the request; this parameter will be filled only after a complete execution process. This parameter encoding is UTF-8 for all languages
Response.TransactionResponseDate	14	Alphanumeric value representing the response date using the following format: ddMMyyyyHHmmss Note: check Appendix A for descriptive details about the date format.
Response.SecureHash	64	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 secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character. The Parameters to use: Response.SecretKey Response.Amount Response.BankID Response.ConfirmationID Response.Currency Response.MerchantId Response.MerchantModuleSessionID Response.Pun Response.Status Response.StatusMessage Response.TransactionResponseDate(ddMMyyyyHHmmss) Example: secretKey = 76a0ed27b643bc6652273f29df66e522 amount = 2300

		bankID = MOFPG420 confirmationID = 140000019886 currency = 784 merchantId = edConnectM merchantModuleSessionID = zI68TI0dYUuucNaJ9Mfo4ZD pun = 1409645751306 status = 0000 statusMessage = Transaction+was+processed+successfully. transactionResponseDate = 02092014100442 The input to the Secure Hash generation routine would be: 76a0ed27b643bc6652273f29df66e5222300MOFPG420140000019886784edConnectMzI68TI0dYUuucNaJ9Mfo4ZD14096457513060000Transaction+was+processed+successfully.02092014100442 Output: 7e1518875613e4848dc03fbbf244e1b1555ccd3faa3360bbfa31cf6e5fea2dce
Response.Amount	12	A numeric value containing the total transaction amount ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100
Response.Currency	3	The numeric ISO Code for the currency and not the character value, e.g.: 840 for US Dollar
Response.MerchantModuleSessionID	256	Alphanumeric value representing the merchant web session id initiating the payment request.
Response.PUN	20	The unique number of the payment order (transaction) generated by the Merchant, it represent a unique identifier for the transaction, and it is alphanumeric.
Response.BankID	10	Alphanumeric value representing e-Dirham System ID, this value is provided by e-Dirham System operation team upon merchant enrollment.

COMPLETION ACTION

For this type of transaction merchant web application handle the communication with e-Dirham System using Back-to-Back Model please refer to section *Communication with EDirham*.
This section describes the main items merchant integrator needs to know to complete pre-authorized transactions, the merchant developer site must be aware that the completion request is only done on authorized transactions only, the merchant developer must flag any authorized transaction for late completion process.

Request

- Merchant collects the Pre-Auth transition information from the transaction that will be completed.
- Generate a HEX encoded HMAC-SHA256 Secure Hash using Merchant's Secret Key.
- Prepare a Request with parameters including the Secure Hash and Pre-Auth information and completion request parameters.
- Send the request as HTTP post to e-Dirham System.

What happens at e-Dirham System side?

- e-Dirham system verifies the request for validity then will process it, if there is an error e-Dirham System will send the error response back, otherwise it will post back the response in the response stream.

The below tables describes all the request parameters that must be collected by merchant site and provided to the PMR POST request link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Mandatory Parameters		
Action	2	Alphanumeric value representing the action to be called 33 for Completion.
MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
Currency	3	The numeric ISO Code for the currency and not the character value, e.g.: 840 for US Dollar
BankID	10	Alphanumeric value representing e-Dirham System ID, this value is provided by e-Dirham System operation team upon merchant enrollment.
TerminalID	8	Alphanumeric value provided by e-Dirham System operation team upon merchant enrollment.
UniqueTransactionID	20	The unique number of the payment order (transaction) generated by the Merchant, it represent a unique identifier for the transaction, and it is alphanumeric.
TransactionRequestDate	14	Alphanumeric value representing the request date time stamp formatted as the following (ddMMyyyyHHmmss).
SecureHash	64	Alphanumeric value representing generated hex-encoded hash using hashing algorithm HMAC-SHA256, by concatenating parameters as a single string starting with the merchant's secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character, null values are not passed to the secure hash, the secret key will be also the key to be passed to the algorithm. The Parameters to use: **`secretKey`** Action BankID Currency Field61_InqAuthCode Field61_InqRRN Field61_InqTrxnId MerchantId TerminalId

		TransactionAmount TransactionRequestDate UniqueTransactionID Example: bankID = MOFPG420 currency = 784 terminalId = 123 uniqueTransactionID = 1409493788914 transactionRequestDate = 31082014170337 transactionAmount = 1600 field61_InqAuthCode = 2 field61_InqRRN = 2 field61_InqTrxnId = 1409493788999 action = 33 merchantId = edConnectM Secret Key: 76a0ed27b643bc6652273f29df66e522 The input to the Secure Hash generation routine would be: **76a0ed27b643bc6652273f29df66e52233MOFPG420784221409493788999edConnectM123160031082014165812140949194923 9** Output: **zJouYq3E3d79DZBMY0LtCNBcNZawM6ouNGEdcsHbVA4=**
TransactionAmount	12	A numeric value containing the total transaction amount ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100
Field61_InqAuthCode	6	The Auth Code returned as part of the pre-authorization request.
Field61_InqRRN	12	The Remote Retrieval Number of the pre-authorization request.
Field61_InqTrxnID	20	The unique transaction Id of the pre-authorization request.

Response

- Merchant site response page receives the response from e-Dirham System
- Verify the received secure hash based on the received parameters.

- Verify the success of execution by checking the response code from the received parameter.
- Apply the required business logic based on the transaction result.

The below tables describes all the request parameters that must be collected by merchant site and provided to the Payment Router POST redirect link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Response.Status	30	Alphanumeric value representing response code, this code covers both errors generated PMR interface e-Dirham System. Please refer to section 5.2 for more details about the response codes values, descriptions and actions to take accordingly.
Response.StatusMessage	512	A string representing a message describing the response status as received from e-Dirham System.
Response.RetrievalRefNumber	15	Alphanumeric value representing a confirmation id generated by e-Dirham System as confirmation reference for the current payment transaction
Response.MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
Response.UniqueTransactionID	20	The unique number of the payment order (transaction) generated by the Merchant, it represent a unique identifier for the transaction, and it is alphanumeric. (returned as in request)
Response.TransactionAmount	12	A numeric value containing the total transaction amount ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100
Response.SecureHash	64	Alphanumeric value representing generated hex-encoded hash using hashing algorithm HMAC-SHA256, by concatenating parameters as a single string starting with the merchant's secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character, null values are not passed to the secure hash, the secret key will be also the key to be passed to the algorithm. **The Parameters to use:** Response.SecretKey Response.MerchantId Response.RetrievalRefNumber Response.Status Response.StatusMessage Response.TransactionAmount Response.TransactionResponseDate(ddMMyyyyHHmm

		ss) Response.UniqueTransactionID **Example:** retrievalRefNumber = 140000019861 uniqueTransactionID = 1409640903408 transactionAmount = transactionResponseDate = 02092014094337 status = 0000 statusMessage = Transaction was processed successfully. secureHash = 09e5803e4054afe916de7b9f5b86654bc95cc2b3873479a09d1daf97b9b50028 merchantId = edConnectM **The input to the Secure Hash generation routine would be:** **76a0ed27b643bc6652273f29df66e522edConnectM1400000198610000Transaction was processed successfully.02092014094337140964090340 8** **Output:** **/xWsl+kIhanbPJPYc42PwXKAhRzOkMCMkpDTHvOACHU=**
Response.TransactionResponseDate	14	Alphanumeric value representing the response date using the following format: ddMMyyyyHHmmss Note: check Appendix A for descriptive details about the date format.

AUTO UPDATE (CONFIRMING TRANSACTION) ACTION

For this type of transaction merchant web application handle the communication with e-Dirham System using Back-to-Back Model please refer section *Communication with EDirham*.
This section describes the main items merchant integrator needs to know to confirm transactions.
The confirm process (known also as auto update) helps the merchant application to:

- Synchronize the status of the requested payments between the merchant and the e-Dirham System records.
- Settle with the e-Dirham System for the transactions processed and hence collect the amounts paid for.

- Guarantee the confirmation of the processed transactions and hence reduce any reversal required.
- Minimize the management of the transactions processing completion on the merchant application and hence requires less development effort.

The execution of the confirm process should be automated using an application with scheduled execution time agreed with e-Dirham System operation team.

Request

- Generate a HEX encoded HMAC-SHA256 Secure Hash using Merchant's Secret Key.
- Send a request as HTTP post to e-Dirham System with the PUN of the transaction to be confirmed with the rest of mandatory parameters.

What happens at e-Dirham System side?

- e-Dirham System verifies the request for validity then will process it, if there is an error e-Dirham System will send the error response back; otherwise it will post back the response in the response stream.

The below tables describes all the request parameters that must be collected by merchant site and provided to the PMR POST request link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Action	2	Alphanumeric value representing the action to be called 13 for Auto Update.
MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
BankID	10	Alphanumeric value representing e-Dirham System ID, this value is provided by e-Dirham System operation team upon merchant enrollment.
PUN	20	The unique transaction Id (PUN) of the original transaction to be Auto Updated, and it is alphanumeric.
TransactionRequestDate	14	Alphanumeric value representing the request date time stamp formatted as the following (ddMMyyyyHHmmss).
SecureHash	64	Alphanumeric value representing generated hex-encoded hash using hashing algorithm HMAC-SHA256, by concatenating parameters as a single string starting with the merchant's secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character, null values are not passed to the secure hash, the secret key will be also the key to be passed to the algorithm. The Parameters to use: secretKey Action BankID MerchantId Pun TransactionRequestDate Example: bankID =MOFPG420 pun =1405934673085 transactionRequestDate =31082014170918 action =13 merchantId =edConnectM Secret Key: 76a0ed27b643bc6652273f29df66e522 The input to the Secure Hash generation routine would

	be: **76a0ed27b643bc6652273f29df66e52213MOFPG420edConnectM1405934673085310820141709 18** Output: Ed0p+w0NlaRhHTauViWdKlQ2BBxmQR0mszsb4VFoTDQ=

Response

- Merchant will receive a response from e-Dirham System
- Verify the received secure hash based on the received parameters.
- Verify the success of execution by checking the response code from the received parameter.
- Apply the required business logic based on the transaction result.

The below tables describes all the request parameters that must be collected by merchant site and provided to the PMR POST request link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Response.Action	2	Alphanumeric value representing the action of the original transaction The action types values can be found in Appendix C, table 16
Response.Status	30	Alphanumeric value representing response code of the request. Please refer to section 5.2 for more details about the response codes values, descriptions and actions to take accordingly.
Response.StatusMessage	512	A string representing a message describing the response status as received from e-Dirham System.
Response. OriginalTransactionStatus	30	Alphanumeric value representing the status of the transaction to be confirmed. Please refer to section 5.2 for more details about the response codes values, descriptions and actions to take accordingly.
Response.OriginalTransactionStatusMessage	512	A string representing a message describing the status of the transaction to be confirmed as received from e-Dirham System.
Response.ConfirmationID	15	Alphanumeric value representing a confirmation id generated by e-Dirham System as confirmation reference for the current payment transaction.
Response.TransactionResponseDate	14	Alphanumeric value representing the response date using the following format: ddMMyyyyHHmmss Note: check Appendix A for descriptive details about the date format.
Response.TransactionAmount	12	A numeric value containing the total transaction amount ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100
Response.BankID	10	Alphanumeric value representing e-Dirham System ID, this value is provided by e-Dirham System operation team upon merchant enrollment.
Response.Currency	3	The numeric ISO Code for the currency and not the character value, e.g.: 840 for US Dollar
Response.ExtractStatus	10	A numeric value representing the extract status of the transaction.

		Extract status to confirm = 0 Extract status to extract = 1 Extract status not to extract = 2 Extract status acknowledged = 3 Extract status cutoff = 4 Extract status unconfirmed = 5
Response.MerchantModuleSessionID	256	Alphanumeric value representing the merchant web session id initiating the payment request.
Response.PUN	20	The unique transaction Id (PUN) of the original transaction to be Auto Updated, and it is alphanumeric.
Response.EDirhamFees	30	An ISO formatted amount containing e-Dirham fees
Response.CollectionCenterFees	30	An ISO formatted amount containing the Collection Center fees.
Response.EServiceData		A JSON string contains information about the e-service data.
Response.SecureHash	64	Alphanumeric value representing generated hex-encoded hash using hashing algorithm HMAC-SHA256, by concatenating parameters as a single string starting with the merchant's secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character, null values are not passed to the secure hash, the secret key will be also the key to be passed to the algorithm. The Parameters to use: Response.SecretKey Response.Action Response.BankID Response.ConfirmationID Response.Currency Response.ExtractStatus Response.MerchantId Response.MerchantModuleSessionID Response.OriginalTransactionStatus Response.OriginalTransactionStatusMessage Response.Pun

	Response.Status Response.StatusMessage Response.TransactionAmount Response.TransactionResponseDate(ddMMyyyyHHmmss) Example: action = 0 originalTransactionStatus = 0000 originalTransactionStatusMessage = Transaction was processed successfully. confirmationID = 140000019338 transactionResponseDate = 02092014095524 transactionAmount = 2300 bankID = MOFPG420 currency = 784 extractStatus = 2 merchantModuleSessionID = 7OtJfgi2hYCj45egK4IHt2d pun = 1409050929296 status = 6514 statusMessage = Auto update: Transaction is already updated. secureHash = 95f60c3421155d8c53da8567777a70a0258e48d10fed1f7173572389fe4e5155 merchantId = edConnectM The input to the Secure Hash generation routine would be: **76a0ed27b643bc6652273f29df66e5220MOFPG4201400001933878427OtJfgi2hYCj45egK4IHt2d0000Transaction was processed successfully14090509292966514Auto update: Transaction is already updated.230002092014095524** Output: **v60kadIvdTvwGcut+iSZEMWai/a+Em+YhmRdEnVfaOY=**

Sample Code For Sending The Request

The below code sample shows how a merchant can send an auto update request to the PMR:

```
    public void doAutoUpdate() throws Exception {
        try {
            String parametersToHash = getParamteresToHash() ;
            String secretKey = "[Value of Merchant Secret Key]";
            String secureHash =
generateHMACSHA256Hash(parametersToHash,secretKey);

            StringBuffer requestQuery = new StringBuffer();

            requestQuery.append("Action").append("=").append("13")
            .append("&").append("MerchantID")
            .append("=").append("[Value of Merchant ID]")
            .append("&").append("BankID")
            .append("=").append("[Value of Bank ID]")
            .append("&").append("PUN")
            .append("=").append("1414414845606")
            .append("&").append("TransactionRequestDate")
            .append("=").append("22012015135919")
            .append("&").append("SecureHash")
            .append("=").append(secureHash);

            String url =

      "http://www.website.com/PaymentRouter/AcceptB2BMessageServlet";

            // Send Post Request
            Map<String, Object> results =
                  sendHttpPost(url, requestQuery.toString());

            // Handle the map that contains the response parameters with
            // their values
        } catch (Exception e) {
            e.printStackTrace();
        }
    }

    private String getParamteresToHash() {
      StringBuffer paramterToHash = new StringBuffer();
      paramterToHash
      .append("[Value of Merchant Secret Key]") // Secret Key
        .append("13") // Auto Update Action
        .append("[Value of Bank ID]") // Bank ID
        .append("[Value of Merchant ID]") // Merchant ID
        .append("1414414845606") // Payment Unique Number (PUN)
        .append("22012015135919"); // Transaction Request Date
```

```
    return paramterToHash.toString();
}

private Map sendHttpPost(String reqUrl, String queryString)
        throws Exception {

    Map mapOutput = null;

    try {
        StringBuffer output = null;

        // Send the request
        URL url = new URL(reqUrl);
        URLConnection conn = url.openConnection();
        conn.setDoOutput(true);
        OutputStreamWriter writer =
              new OutputStreamWriter(conn.getOutputStream());

        //write parameters
        writer.write(queryString);
        writer.flush();

        // Get the response
        output = new StringBuffer();
        BufferedReader reader =
              new BufferedReader(
                          new InputStreamReader(conn.getInputStream(),
                                      "UTF-8"));

        String line;
        while ((line = reader.readLine()) != null) {
            output.append(line);
        }
        writer.close();
        reader.close();

        mapOutput =
              parseStringToMap(output.toString(), "&", true);

    } catch (MalformedURLException e) {
        e.printStackTrace();
    } catch (IOException e) {
        e.printStackTrace();
    }

    return mapOutput;
}
```

```
    private Map<String, String> parseStringToMap(String src,
            String separator, boolean handleAndSign) throws Exception {
        Map<String, String> nameValuePair =
            new HashMap<String, String>();

        if (src != null && src.trim().length() > 0) {
            String          name                    = null;
            String          value                   = null;

            String []namesValues =  src.toString().split(separator);

            for(String nameValue: namesValues) {

                if(nameValue.indexOf("=") == -1) {
                    value =
                        new StringBuilder (nameValuePair.get(name))
                        .append(separator).append(nameValue).toString();
                } else {
                    name = nameValue.substring(0, nameValue.indexOf("="));
                    value = nameValue.substring(nameValue.indexOf("=") + 1);
                }

                // If value contains //& then replace back with &
                if (handleAndSign && value.indexOf("//&") != -1) {
                    value = value.replaceAll("//&", "&");
                }

                nameValuePair.put(name, value);
            }
        }

        return nameValuePair;
    }

              String generateHMACSHA256Hash(String data, String
merchantSecretKey) {
        String result = "";

            {
            String HMAC_SHA256_ALGORITHM = "HmacSHA256";

            // Get an HMAC SHA256 key from the raw key bytes
            SecretKeySpec signingKey =
SecretKeySpec(merchantSecretKey.getBytes(), HMAC_SHA256_ALGORITHM);

            // Get an HMAC SHA256 Mac instance and initialize with the
signing key
            Mac mac = Mac.getInstance(HMAC_SHA256_ALGORITHM);
            mac.init(signingKey);
```

```
            // Compute the HMAC on input data bytes
                [] rawHmac = mac.doFinal(data.getBytes());

            // Convert to hexadecimal
            result = Hex.encodeHexString(rawHmac);

            // Base64-encode the HMAC
            result =     String(Base64.encodeBase64(result.getBytes()));
        }       (NoSuchAlgorithmException e) {
            e.printStackTrace();
        }       (InvalidKeyException e) {
            e.printStackTrace();
        }

                result;
    }
```

REFUND

For this type of transaction merchant web application handle the communication with e-Dirham System using Back-to-Back Model please refer to section *Communication with EDirham*.
Refund is used to return the money back to the customer after he performed completed successful transaction and for some reason the customer want to cancel the transition. Refund can be performed for the full amount of the original transaction or partial amount without the transaction fees, where the total refunded amount cannot exceed the original transaction amount, and only a successful payment transaction can be refunded.
The initiator of the refund transaction should be a privileged merchant administrator aware of the refund reason and the valid cases for refunding transactions.
Note: The e-Dirham System may not be enabled to process the Refund function based on the business functionality requirements of e-Dirham System. Please refer to e-Dirham System

operation team for more information regarding Refund function being supported by e-Dirham System or not.

Request

This section describes in details the integration process required to refund transactions, and listing all the required parameters.

- Merchant collects the e-Service to be refunded information from the original transaction.
- Generate a HEX encoded HMAC-SHA256 Secure Hash using Merchant's Secret Key.
- Prepare a Request with parameters including the Secure Hash and e-Service information the rest of request parameters.
- Send the request as HTTP POST to e-Dirham System.

What happens at e-Dirham System side?

- e-Dirham System verifies the request for validity then will process it, if there is an error e-Dirham System will send the error response back, otherwise it will post back the response in the response stream.

The below tables describes all the request parameters that must be collected by merchant site and provided to the PMR POST request link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Mandatory Parameters		
Action	2	Alphanumeric value representing the action to be called 37 for Refund.
BankID	10	Alphanumeric value representing e-Dirham System ID, this value is provided by e-Dirham System operation team upon merchant enrollment.
MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
TerminalID	8	Alphanumeric value provided by e-Dirham System operation team upon merchant enrollment.
TransactionRequestDate	14	Alphanumeric value representing the reques: date time stamp formatted as the following (ddMMyyyyHHmmss).
Currency	3	The numeric ISO Code for the currency and not the character value, e.g.: 840 for US Dollar
UniqueTransactionID	20	The unique identifier of the refund transaction generated by the Merchant, it represent a unique identifier for the transaction, and it is alphanumeric.
Field63_OriginalTransactionUniqueID	20	The unique transaction Id of the Original transaction and it is alphanumeric.
Field61_ServiceMainCodeSubCode	12	The main code-sub code of the e-service to refund.
Field61_ServiceCodeQuantity	2	The quantity used in the e-service inquiry request.
TransactionAmount	12	A numeric value containing total amount of the transaction to be refunded ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100
SecureHash	64	Alphanumeric value representing generated hex-encoded hash using hashing algorithm HMAC-SHA256, by concatenating parameters as a single string starting with the merchant's secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character**, null values are not passed to the secure hash, the secret key will be also the key to be passed to the algorithm.**

The Parameters to use:

- secretKey
- Action
- BankId
- Currency
- Field61_ServiceCodeQuantity
- Field61_ServiceMainCodeSubCode
- Field63_OriginalTransactionUniqueId
- MerchantId
- TerminalId
- TransactionAmount
- TransactionRequestDate
- UniqueTransactionId

Example:

- bankId =MOFPG420
- terminalId =123
- transactionRequestDate =31082014170839
- currency =784
- uniqueTransactionId =1409494111485
- field63_OriginalTransactionUniqueId =1404376514678
- field61_ServiceMainCodeSubCode =000000-0002
- field61_ServiceCodeQuantity =1
- transactionAmount =2300
- action =37
- merchantId =edConnectM
- Secret Key: 76a0ed27b643bc6652273f29df66e522
-

The input to the Secure Hash generation routine would be:

- `76a0ed27b643bc6652273f29df66e52237MOFPG4207841000000-00021404376514678edConnectM123230031082014170839140949411148 5`

Output:

- `fdBzwiRtDj3WJ7GseyIOR4h5QWC/tD1uzsKC/vkawR8=`

Response

- Merchant will receive a response from e-Dirham System
- Verify the received secure hash based on the received parameters.
- Verify the success of execution by checking the response code from the received parameter.
- Apply the required business logic based on the transaction result.

The below tables describes all the request parameters that must be collected by merchant site and provided to the PMR POST request link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Response.Status	30	Alphanumeric value representing response code of the request. Please refer to section 5.2 for more details about the response codes values, descriptions and actions to take accordingly.
Response.StatusMessage	512	A string representing a message describing the response status as received from e-Dirham System.
Response.RetrievalRefNumber	15	Alphanumeric value representing a confirmation id generated by e-Dirham System as confirmation reference for the current payment transaction.
Response.UniqueTransactionID	20	The unique number of the payment order (transaction) generated by the Merchant, it represent a unique identifier for the transaction, and it is alphanumeric. (returned as in request)
Response.MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
Response.TransactionAmount	12	A numeric value containing total amount of the transaction to be refunded ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100
Response.TransactionResponseDate	14	Alphanumeric value representing the response date using the following format: ddMMyyyyHHmmss Note: check Appendix A for descriptive details about the date format.
Response.SecureHash	64	**Alphanumeric value representing generated hex-encoded hash using hashing algorithm HMAC-SHA256, by concatenating parameters as a single string starting with the merchant's secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character, , null values are not passed to the secure hash, the secret key will be also the key to be passed to the algorithm.** The Parameters to use: Response.SecretKey Response.MerchantId

Response.RetrievalRefNumber

Response.Status

Response.StatusMessage

Response.TransactionAmount

Response.TransactionResponseDate(ddMMyyyyHHmmss)

Response.UniqueTransactionId

Example:

retrievalRefNumber = 140000019867

uniqueTransactionId = 1409642041365

transactionAmount =

transactionResponseDate = 02092014100300

status = 0000

statusMessage = Transaction was processed successfully.

secureHash = 4892b5db3501b37f56407e9b4273e1f53a9de0b546e288126bc6166033ed01a5

merchantId = edConnectM

The input to the Secure Hash generation routine would be:

```
76a0ed27b643bc6652273f29df66e522edConnectM1400000198670000Transaction was processed successfully.02092014100300140964204136
```

Output:

```
JeJ6sO4votaUhDUfbtHGYKsCV6X91HrDXl2C282Jro4=
```

VOID

For this type of transaction merchant web application handle the communication with e-Dirham System using Back-to-Back Model please refer to section **Error! Reference source not found.***Communication with EDirham*.

Void sale is used to discard any payment action such as (Sale/Authorize/Completion), in this way; the original transaction will be voided completely including the Fees.

The initiator of the void transaction should be a privileged merchant administrator aware of the void reason and the valid cases for voiding transactions. In some merchant implementations the

decision of making void is taken by the merchant web application automatically (no human interaction) where the web application is aware of any service delivery failure to the customer after he performed the payment transaction successfully.
Void transactions needs preapproval from a merchant admin.

Note: The e-Dirham System may not be enabled to process the Refund function based on the business functionality requirements of e-Dirham System. Please refer to e-Dirham System operation team for more information regarding Refund function being supported by e-Dirham System or not.

Request

This section describes in details the integration process required to void transactions, and listing all the required parameters

- Merchant collects the transaction information to be voided.
- Generate a HEX encoded HMAC-SHA256 Secure Hash using Merchant's Secret Key.
- Prepare a Request with parameters including the Secure Hash and transaction information the rest of request parameters.
- Send the request as HTTP POST to e-Dirham System.

What happens at e-Dirham System side?

- e-Dirham System verifies the request for validity then will process it, if there is an error e-Dirham System will send the error response back, otherwise it will post back the response in the response stream.

The below tables describes all the request parameters that must be collected by merchant site and provided to the Payment Router POST request link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Mandatory Parameters		
Action	2	Alphanumeric value representing the action to be called 30 for eService inquiry.
BankID	10	Alphanumeric value representing e-Dirham System ID, this value is provided by e-Dirham System operation team upon merchant enrollment.
MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
TerminalID	8	Alphanumeric value provided by e-Dirham System operation team upon merchant enrollment.
TransactionRequestDate	14	Alphanumeric value representing the request date time stamp formatted as the following (ddMMyyyyHHmmss).
Currency	3	The numeric ISO Code for the currency and not the character value, e.g.: 840 for US Dollar
UniqueTransactionID	20	The unique number of the payment order (transaction) generated by the Merchant, it represent a unique identifier for the transaction, and it is alphanumeric.
Field63_OriginalTransactionUniqueID	20	The unique transaction Id of the Original transaction and it is alphanumeric.
TransactionAmount	12	A numeric value containing total amount of the transaction to be voided ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100
SecureHash	64	**Alphanumeric value representing generated hex-encoded hash using hashing algorithm HMAC-SHA256, by concatenating parameters as a single string starting with the merchant's secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character,** null values are not passed to the secure hash, the secret key will be also the key to be passed to the algorithm.

The Parameters to use:

- secretKey
- Action
  BankId
  Currency
  Field63_OriginalTransactionUniqueId
  MerchantId
  TerminalId
  TransactionAmount
  TransactionRequestDate
  UniqueTransactionId

Example:

- bankId = MOFPG420
- terminalId = 123
- transactionRequestDate = 31082014171209
- currency = 784
- uniqueTransactionId = 1409494322362
- field63_OriginalTransactionUniqueId = 1408445906893
- transactionAmount = 2300
- action = 30
- merchantId = edConnectM
- Secret Key: 76a0ed27b643bc6652273f29df66e522

The input to the Secure Hash generation routine would be:

```
76a0ed27b643bc6652273f29df66e52230MOFPG420784140437651467 8edConnectM123230031082014171209140949432 2362
```

Output:

```
IWWhyGlxqNgXYB8pB34dWQTdrQOg79UoBgeSR3rUaRI=
```

Response

- Merchant will receive a response from e-Dirham System
- Verify the received secure hash based on the received parameters.
- Verify the success of execution by checking the response code from the received parameter.
- Apply the required business logic based on the transaction result.

The below tables describes all the request parameters that must be collected by merchant site and provided to the Payment Router POST request link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Response.Status	30	Alphanumeric value representing response code of the request. Please refer to section 5.2 for more details about the response codes values, descriptions and actions to take accordingly.
Response.StatusMessage	512	A string representing a message describing the response status as received from e-Dirham System.
Response.RetrievalRefNumber	15	Alphanumeric value representing a confirmation id generated by e-Dirham System as confirmation reference for the current payment transaction.
Response.UniqueTransactionID	20	The unique number of the payment order (transaction) generated by the Merchant, it represent a unique identifier for the transaction, and it is alphanumeric. (returned as in request)
Response.MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
Response.TransactionAmount	12	A numeric value containing total amount of the transaction to be refunded ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100
Response.TransactionResponseDate	14	Alphanumeric value representing the response date using the following format: ddMMyyyyHHmmss Note: check Appendix A for descriptive details about the date format.
Response.SecureHash	64	**Alphanumeric value representing generated hex-encoded hash using hashing algorithm HMAC-SHA256, by concatenating parameters as a single string starting with the merchant's secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character, null values are not passed to the secure hash, the secret key will be also the key to be passed to the algorithm.** The Parameters to use: Response.SecretKey Response.MerchantId

	Response.RetrievalRefNumber Response.Status Response.StatusMessage Response.TransactionAmount Response.TransactionResponseDate(ddMMyyyyHHmmss) Response.UniqueTransactionId Example: retrievalRefNumber = 140000019871 uniqueTransactionId = 1409642738725 transactionAmount = transactionResponseDate = 02092014101414 status = 0000 statusMessage = Transaction was processed successfully. secureHash = b3c5e4c193259c3d5dd36bde2c2d629272d97d93d89b84996987e694b7e02ef1 merchantId = edConnectM The input to the Secure Hash generation routine would be: **76a0ed27b643bc6652273f29df66e522edConnectM1400000198670000Transaction was processed successfully.020920141003001409494322362** Output: **v30I9iIcgqxeTT0fOBQU5tPAP2l2n+MaefugJjsGqZs=**

E-DEBIT PAYMENT ACTION

For this type of transaction merchant web application handle the communication with e-Dirham System using Redirect Model please refer to section *Communication with EDirham*.
This section describes the main items merchant integrator needs to know, for building pages integrating merchant web application with e-Dirham System through Payment Router in order to perform e-Debit payment transactions.

Request

- Collect the payment information from the customer with the information of the Inquired e-Service/s or provide extra details if no e-Service inquiry is performed.
- Submit the request to e-Dirham System using Redirect HTTP POST using the provided Redirect Link.

The below tables describes all the request parameters that must be collected by merchant site and provided to the PMR POST redirect link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Mandatory Parameters		
Action	2	Alphanumeric value representing the action to be called, 19 for all e-Debit transactions.
EDebitActionType	-	Alphabetic value represents the specific e-Debit action, value for redirect payment is “Pay” (without quotes).
BankID	10	Alphanumeric value representing e-Dirham System ID, this value is provided by e-Dirham System operation team upon merchant enrollment.
MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
Currency	3	The numeric ISO Code for the currency and not the character value, e.g.: 840 for US Dollar
PUN	20	The unique number of the payment order (transaction) generated by the Merchant, it represent a unique identifier for the transaction, and it is alphanumeric.
PaymentDescription	255	Alphanumeric string containing a narrative description of the payment order using the language specified in the language parameter. This value should be HTML encoded.
MerchantModuleSessionID	256	Alphanumeric value representing the merchant web session id initiating the payment request.
TransactionRequestDate	14	Alphanumeric value representing the request date time stamp formatted as the following (ddMMyyyyHHmmss).
SecureHash	64	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 secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character. The Parameters to use: **secretKey** **Action** **BankId** **Currency** **Amount** **ExtraFields_f17** **ExtraFields_f16**

ExtraFields_f18
Lang
MerchantId
MerchantModuleSessionId
NationalId
PaymentDescription
Pun
TransactionRequestDate
Version

Example:

MerchantID =edConnectM
Action =19
Lang =en
BankID =MOFPG420
Currency =784
MerchantModuleSessionID =jIHDpGpgP7O3pvvtHgrj_kt
PaymentDescription =PaymentRouter+Sample+Payment
ExtraFields_f18 =123
ExtraFields_f17 =1409491949239
ExtraFields_f16 =6-14
PUN =1409492646898
NationalID =8897871212
Amount =2300
TransactionRequestDate =31082014165104
Secret Key: 76a0ed27b643bc6652273f29df66e522

The input to the Secure Hash generation routine would be:

```
76a0ed27b643bc6652273f29df66e5220MOFPG4207842
30014094919492391-
1123enedConnectMjIHDpGpgP7O3pvvtHgrj_kt889787
1212PaymentRouter Sample
Payment14094926468983108201416510 4null
```

Output:

```
c3e0538fa3638be8ed86c86ec7d4c445c04ff9bcdf864
54821ff15c34543947f
```

OR

secretKey
Action
BankId
Currency
ApplicationNumber
ExtraFields_intendedEDirhamService
MainCodeSubCode
Quantity
Price
ExtraFields_f16
ExtraFields_f18
Lang
MerchantId
MerchantModuleSessionId
NationalId
PaymentDescription
Pun
TransactionRequestDate
Version

Example:
MerchantID = edConnectM
Action = 19
ExtraFields_intendedEDirhamService = 0
Lang = en
BankID = MOFPG420
Currency = 784
EServiceMainCodeSubCode_1 = 000000-0002
MerchantModuleSessionID = jIHDpGpgP7O3pvvtHgrj_kt
PaymentDescription = PaymentRouter+Sample+Payment
ExtraFields_f18 = 123
ExtraFields_f16 = 6-14
PUN = 1409493438621
EServiceQuantity_1 = 1

		NationalID = 8897871212 ApplicationNumber = 123 TransactionRequestDate = 31082014165812 Secret Key: 76a0ed27b643bc6652273f29df66e522 The input to the Secure Hash generation routine would be: 76a0ed27b643bc6652273f29df66e5220MOFPG4207841230000000-00021null1-1123enedConnectMjIHDpGpgP7O3pvvtHgrj_kt8897871212PaymentRouter Sample Payment14094934386213108201416581 2null Output: a7991bf81a87c04b3b693e43a6ba8b92876c652939ff933372b8ce11181d5c8e
ExtraFields_f16	3	Payment method type: 6-14: E-Debit Account
ExtraFields_f18	8	The Terminal Id that was assigned to the merchant during the enrollment process for use with e-commerce transactions.
Optional parameters		
ExtraFields_f14	512	Merchant site response page URL that will receive the response from e-Dirham System, this can help merchant having different response pages based on the requested service or any other criteria.
NationalID	32	Alphanumeric value representing the national id of the customer performing the transaction. If this field is not required to be filled by e-Dirham System, it can be set to Empty String: “”. Please consult e-Dirham System operation team for more information.
Lang	2	Alphabetic value representing the language of the interface displayed to customer at merchant site, and used as language for the payment description parameter. e-Dirham System will use this value to display the interface supporting selected language to the customer during the payment process. Supported values are: En Ar
Conditional Parameters		
Option 1		
ExtraFields_f17	20	E-Service inquiry unique transaction Id.

Amount	12	A numeric value containing the total transaction amount ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100
Option 2		
ApplicationNumber	20	Alphanumeric value provided by the merchant.
ExtraFields_intendedEDirham Service	2	The intended e-Dirham Service that is going to be executed after the e-Service inquiry. Expected values: 19: e-Debit Pay
e-Service Details parameters, Mandatory		
The e-Service inquiry request can handle multiple eservices in one request, and for all the details of an e-Service the parameter should be concatenated with a number starting with one for service 1 and 2 for service 2 … etc. **Ex: Sending a request with two e-Services with information as the following:** **e-Service 1: Code=000000-0001, Price=10, Quantity=2** **e-Service 2: Code=000000-0002, Quantity=4** **The request parameters should be added as the following:** **EServiceMainCodeSubCode_1 = 000000-0001, EServiceQuantity_1 = 2, EServicePrice_1 = 10** **EServiceMainCodeSubCode_2 = 000000-0002, EServiceQuantity_2 = 4**		
EServiceMainCodeSubCode_*	12	An alphanumeric value representing the e-Service MainCode-SubCode as XXXXXX-XXXX * Should be replaced with a number for each e-Service group
EServicePrice_*	12	A numeric value representing the price of an eService, this parameter is used only for a ZERO amount e-Service. The value should be ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100 * Should be replaced with a number for each e-Service group
EServiceQuantity_*	6	A numeric value representing the quantity required for each eService. * Should be replaced with a number for each e-Service group

Optional Parameters		
Version	1	Alphanumeric value representing the version of the action to execute (1.0 is the default).

Response

The below tables describes the parameters for the e-Debit Pay Web action, all the parameters are case sensitive without whitespaces

- Merchant site response page receives the response from e-Dirham System.
- Verify the received secure hash based on the received parameters.
- Verify the success of execution by checking the response code from the received parameter.
- Apply the required business logic based on the transaction result.

The below tables describes all the response parameters posted back from e-Dirham System, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Response.Status	30	Alphanumeric value representing the response code, this code covers both errors generated PMR interface e-Dirham System. Please refer to section 5.2 for more details about the response codes values, descriptions and actions to take accordingly.
Response.ConfirmationID	15	Alphanumeric value representing a confirmation id generated by e-Dirham System as confirmation reference for the current payment transaction
Response.StatusMessage	512	Alphanumeric value representing a message describing the response status as received from e-Dirham System using the language specified in the request; this parameter will be filled only after a complete execution process. This parameter encoding is UTF-8 for all languages
Response.TransactionResponseDate	14	Alphanumeric value representing the response date using the following format: ddMMyyyyHHmmss Note: check Appendix A for descriptive details about the date format.
Response.SecureHash	64	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 secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character. The Parameters to use: secretKey Response.Amount Response.BankID Response.CollectionCenterFees Response.ConfirmationID Response.Currency Response.EDirhamFees Response.EServiceData merchantId Response.MerchantModuleSessionID Response.RES_PAYMENT_METHOD_TYPE Response.PUN Response.Status Response.StatusMessage Response.TransactionResponseDate

		Response.TerminalID Example: 76a0ed27b643bc6652273f29df66e5222300MOFPG4202001 0002'],'price':['1000'],'amountWithFees':[1000],'quantity':[' 114109611962810000Transaction+was+processed+successf The input to the Secure Hash generation routine would be: Output: **0098f748ed429cbcc5d00363ab0c862fee622744785270d1 1df833e3fac3145d**
Response.Amount	12	A numeric value containing the total transaction amount ISO Formatted with no decimal point, e.g.: 1.00 USD sent as 100
Response.Currency	**3**	The numeric ISO Code for the currency and not the character value, e.g.: 840 for US Dollar
Response.MerchantModuleSessionID	**256**	Alphanumeric value representing the merchant web session id initiating the payment request.
Response.PUN	**20**	The unique number of the payment order (transaction) generated by the Merchant, it represent a unique identifier for the transaction, and it is alphanumeric.
Response.BankID	**10**	Alphanumeric value representing e-Dirham System ID, this value is provided by e-Dirham System operation team upon merchant enrollment.
Response.TerminalID	**8**	The Terminal Id that was assigned to the merchant during the enrollment process to use it with e-commerce transactions.
Response.ReceiptID	**15**	Alphanumeric value representing a receipt id generated by eD-Wallet System as receipt reference for the current payment transaction
Response.CollectionCenterFees	**12**	A numeric value containing a collection center fees ISO Formatted with no decimal point, e.g.: 1.00 AED sent as 100
Response.EDirhamFees	**12**	A numeric value containing an eDirham fees ISO Formatted with no decimal point, e.g.: 1.00 AED sent as 100
Response.TransactionAmount	**12**	A numeric value containing the total transaction amount ISO Formatted with no decimal point, e.g.: 1.00 AED sent as 100
Response.EServiceData		

mainSubCode	12	An alphanumeric value representing the e-Service MainCode-SubCode as XXXXXX-XXXX Ex: 000000-0001
price	12	A numeric value representing the price of an eService, this parameter is used only for a ZERO amount e-Service. The value should be sent normaly as the Price value as 22.55 AED
quantity	6	A numeric value representing the quantity for each eService.
ownerFees	12	A numeric value containing an owner fees ISO Formatted with no decimal point, e.g.: 1.00 AED sent as 100
amountWithoutFees	12	A numeric value containing the total amount for a specific service (price*quantity) exclude the owner fees The amount must be formatted as ISO Formatt with no decimal point, e.g.: 1.00 AED sent as 100
amountWithFees	12	A numeric value containing the total amount for a specific service (price*quantity+ownerFees) include the owner fees The amount must be formatted as ISO Formatt with no decimal point, e.g.: 1.00 AED sent as 100

All payment request parameters passed as simple parameters except the eService details(if exist), it must be passed as JSON array object as follow:

EServiceData:

```
[
   {
      "mainSubCode": "000000-0005",
      "price": "",
      "quantity": "1"
   },
   {
      "mainSubCode": "000000-0001",
      "price": "",
      "quantity": "1"
   },
   {
      "mainSubCode": "000000-0002",
      "price": "22.25",
      "quantity": "1"
   }
]
```

Figure 3 EServiceData Parameter sample

E-DEBIT STATUS DELIVERY

For this type of transaction merchant web application handle the communication with e-Dirham System using Back-to-Back Model please refer to section *Communication with EDirham*.
e-Debit Status Delivery is used to confirm, reverse or void an e-Debit transaction.

Request

This section describes in details the integration process required to confirm, reverse or void the e-Debit transaction, and listing all the required parameters.

- Merchant collects the payment unique number for the original transaction.
- Generate a HEX encoded SHA2 Secure Hash using Merchant's Secret Key and other parameters.
- Prepare a Request with parameters including the Secure Hash, the payment unique number, and the rest of request parameters.
- Send the request as HTTP POST to e-Dirham System.

What happens at e-Dirham System side?

- e-Dirham System verifies the request for validity then will process it, if there is an error e-Dirham System will send the error response back, otherwise it will post back the response in the response stream.

The below tables describes all the request parameters that must be collected by merchant site and provided to the PMR POST request link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Mandatory Parameters		
Action	2	Alphanumeric value representing the action to be called, 19 for all e-Debit transactions.
EDebitActionType	-	Alphabetic value represents the specific e-Debit action, value for status delivery is "Delivery" (without quotes).
MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
PUN	20	The unique transaction ID of the original e-Debit transaction and it is alphanumeric.
TransactionRequestDate	14	Alphanumeric value representing the request date time stamp formatted as the following (ddMMyyyyHHmmss).
DeliveryStatus	10	Alphabetic value represents the delivery status. Allowed values are: • CONFIRM • REVERSAL • VOID
SecureHash	64	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 secret key, then other values in the following order, with no separators and no terminating character. The Parameters to use: • SecretKey • EDebitActionType • MerchantID • PUN • TransactionRequestDate • DeliveryStatus Example: • EDebitActionType =Delivery • MerchantID =edConnectM • PUN =1409494111485 • TransactionRequestDate =31082014170839

- DeliveryStatus = CONFIRM
- SecretKey: 76a0ed27b643bc6652273f29df66e522

The input to the Secure Hash generation routine would be:

- 76a0ed27b643bc6652273f29df66e522DeliveryedConnectM1409494111485310820 14170839CONFIRM

Output:

- e8f956795070c9f9c61b1e9b597bd50c3d a1dbd643ead7358de8610a0cd8db8b

Response

- Merchant will receive a response from e-Dirham System
- Verify the received secure hash based on the received parameters.
- Verify the status of execution by checking the response code from the received parameter.
- Apply the required business logic based on the transaction result.

The below tables describes all the request parameters that must be collected by merchant site and provided to the PMR POST request link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Response.Status	30	Alphanumeric value representing response code of the request.
Response.StatusMessage	512	A string representing a message describing the response status as received from e-Dirham System.
Response.MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
Response.SettlementDate	8	A date supplied by the Central Bank Payment Gateway to indicate when this transaction will be settled, in the format ***yyyyMMdd***, e.g: 20150217
Response.SecureHash	64	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 secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character. The Parameters to use: SecretKey Response.MerchantID Response.Status Response.StatusMessage Example: MerchantID = edConnectM Status = 0000 StatusMessage = Transaction was processed successfully. SecretKey: 76a0ed27b643bc6652273f29df66e522 SecureHash = 23e6177660648948b02b0019b383facd08a88722cfeb5cea7588da652e30ced7 The input to the Secure Hash generation routine would be: 76a0ed27b643bc6652273f29df66e522edConnectM0000Transaction was processed successfully. Output:

	23e6177660648948b02b0019b383facd08a88722cfeb5cea7588da652e30ced7

E-DEBIT STATUS UPDATE

For this type of transaction merchant web application handle the communication with e-Dirham System using Back-to-Back Model please refer to section *Communication with EDirham*.
e-Debit Status Update is used to inquire or update the e-Debit transaction status.

Request

This section describes in details the integration process required to inquire or update the e-Debit transaction status, and listing all the required parameters.

- Merchant collects the payment unique number for the original transaction.
- Generate a HEX encoded SHA2 Secure Hash using Merchant's Secret Key and other parameters.
- Prepare a Request with parameters including the Secure Hash, the payment unique number, and the rest of request parameters.
- Send the request as HTTP POST to e-Dirham System.

What happens at e-Dirham System side?

- e-Dirham System verifies the request for validity then will process it, if there is an error e-Dirham System will send the error response back, otherwise it will post back the response in the response stream.

The below tables describes all the request parameters that must be collected by merchant site and provided to the PMR POST request link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Mandatory Parameters		
Action	2	Alphanumeric value representing the action to be called, 19 for all e-Debit transactions.
EDebitActionType		Alphabetic value represents the specific e-Debit action, value for status update is “Inquiry” (without quotes).
MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
PUN	20	The unique transaction ID of the original e-Debit transaction and it is alphanumeric.
TransactionRequestDate	14	Alphanumeric value representing the request date time stamp formatted as the following (ddMMyyyyHHmmss).
SecureHash	64	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 secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character. The Parameters to use: • SecretKey • EDebitActionType • MerchantID • PUN • TransactionRequestDate Example: • EDebitActionType = Inquiry • MerchantID =edConnectM • PUN =1409494111485 • TransactionRequestDate =31082014170839 • SecretKey: 76a0ed27b643bc6652273f29df66e522 The input to the Secure Hash generation routine would be: • 76a0ed27b643bc6652273f29df66e522Inq

uiryedConnectM14094941114853108201 4170839

Output:

- 717fdd8f7899e85e8c439c4e4136a62429 b1fbdef43cf9ae86f328654dd7dc23

Response

- Merchant will receive a response from e-Dirham System
- Verify the received secure hash based on the received parameters.
- Verify the status of execution by checking the response code from the received parameter.
- Apply the required business logic based on the transaction result.

The below tables describes all the request parameters that must be collected by merchant site and provided to the PMR POST request link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Response.Status	30	Alphanumeric value representing response code of the request.
Response.StatusMessage	512	A string representing a message describing the response status as received from e-Dirham System.
Response.MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
Response.RetrievalRefNumber	12	A unique number generated by the Central Bank Payment Gateway at the time of transaction processing
Response.SettlementDate	8	A date supplied by the Central Bank Payment Gateway to indicate when this transaction will be settled, in the format ***yyyyMMdd***, e.g: 20150217
Response.AuthCode	6	An identifying code issued by the issuing bank to approve or deny the transaction.
Response.SettlementExpiry	14	A date supplied by the Payment Gateway indicating that if the merchant does not send a Confirmation of the transaction by this time, the PG will mark the transaction as expired and the Merchant will not be able to resume it, in the format ***yyyyMMddHHmmss***, e.g: 20150217134055
Response.SecureHash	64	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 secret key, then each data field in ascending alphabetical order of that field name, with no separators and no terminating character. The Parameters to use: SecretKey Response.MerchantID Response.Status Response.StatusMessage Example: MerchantID = edConnectM Status = 0000 StatusMessage = Transaction was processed successfully.

	SecretKey: 76a0ed27b643bc6652273f29df66e522 SecureHash = 23e6177660648948b02b0019b383facd08a88722cfeb5cea7588da652e30ced7 The input to the Secure Hash generation routine would be: 76a0ed27b643bc6652273f29df66e522edConnectM0000Transaction was processed successfully. Output: 23e6177660648948b02b0019b383facd08a88722cfeb5cea7588da652e30ced7

E-DIRECT TOP-UP G2 CARD FROM BANK ACCOUNT

This service is used to top-up G2 card from bank account. It will take the user to eDirect module pages without response back to merchant.
This section describes the main items merchant integrator needs to know, for building pages integrating merchant web application with e-Dirham System(eDirect Module) through Payment Router in order to perform top-up G2 card from bank account.

Request

The below tables describes all the request parameters that must be collected by merchant site and provided to the PMR POST request link, all the parameters are case sensitive without whitespaces.

Parameter Name	Length	Description
Mandatory Parameters		
MerchantID	10	Alphanumeric value representing the unique id of the merchant at e-Dirham System, this value is provided by e-Dirham System operation team upon merchant enrollment.
Lang	2	Alphabetic value representing the language of the interface displayed to customer. Supported values are (en ,ar).
Optional parameters		
CardNo	16	Numeric value representing card number. If USER not logged in the system "Empty String".
Passcode	8	Alphanumeric value representing passcode. If USER not logged in the system "Empty String".

APPENDICES

Appendix A: Date Format

The full description of the letter used in the format of any date parameter in this document is described below.

Table 1: Date Format

Letters	Usage	Example
yyyy	Year	2009
MM	Month in year (01-12)	09
dd	Day in month (01-31)	27
HH	Hour in day (00-23)	16
mm	Minute in hour (00-59)	50
ss	Second in minute (00-59)	15
S	Millisecond	8

Appendix B: Response codes

Payment and Pre-Auth Response Codes

Table 2: Payment and Pre-Auth Response Codes

Status Code	Description	Action to take
EDConnect Error Codes		
EDConnect-0000	Missing "TransactionRequestDate" Parameter	Provide the missing parameter
EDConnect-0024	Merchant has no configured secret key	The merchant admin should configure a Secret Key and use it in the Hashing routine
EDConnect-0029	Missing "SecureHash" parameter	Provide the missing parameter
EDConnect-0030	Secure Hash Could not be validated	Check the parameters used to hash, and recheck the routine in the request parameters
e-Dirham System Error Codes		
0000	Payment was processed successfully	Requires confirmation
0001	Transaction is completed successfully but early auto update failed	Requires confirmation, Contact e-Dirham System operator for support
2000	Bank ID received not available	Provide e-Dirham System bank ID provided by operation team
2001	Merchant reply address is invalid, it does not match the one configured for the merchant	Requires confirmation, Contact e-Dirham System operator for support
2005	Merchant is either set to inactive on e-Dirham System side or its contract has expired	Requires confirmation, Contact e-Dirham System operator for support
2010	Merchant is not configured to accept payment in the current transaction's currency	Requires confirmation, Contact e-Dirham System operator for support
2011	PUN for payment already exists on e-Dirham System	Requires confirmation, Send the payment transaction with a different PUN
2016	Message signature could not be verified	Requires confirmation, Make sure you shared the proper Public Certificate with e-Dirham System, or

		that you are using the appropriate Private Key for signing transactions
2027	Action provided with the transaction is either invalid or the merchant is not configured to support it	Requires confirmation, Contact e-Dirham System operator for support
2028	One of the transaction mandatory parameters is missing	Requires confirmation, Provide the missing data
2029	Transaction is not safe against e-Dirham System risk rules	Requires confirmation, Contact e-Dirham System operator for support
2030	Transaction is not safe against Merchant risk rules	Requires confirmation, Contact e-Dirham System operator for support
2033	Amount value contains decimal value	Requires confirmation, Provide the correct amount format
2034	Amount value is zero	Requires confirmation, Provide the correct amount.
2035	Amount value has exceeded limit	Requires confirmation, Provide the correct amount.
2036	PUN for payment already exists on e-Dirham System	Requires confirmation, Send the payment transaction with a different PUN
2042	One of the transaction mandatory parameters is missing	Requires confirmation, Provide the missing data
2046	Request timed out at the backend side	Requires confirmation, Attempt payment again later on
2048	Payment method selected, this is an intermediate status code, it will change as the transaction progresses, the merchant should not receive this status ever	-
2090	Terminal ID mismatch	Contact e-Dirham System operator for support
2091	Amount does not match eService Inquiry amount	Requires confirmation, Provide the correct amount.
2092	Payment method is not supported by merchant	Requires confirmation, Contact e-Dirham System operator for support
2094	Intended e-Dirham Service Mismatch	Provide the right intended e-

		dirham service
2097	Timeout exceeded between eService Inquiry and payment	Requires confirmation, Payment should be repeated
2102	Not Payment Router Merchant.	
2898	Request URL does not match merchants configurations	Requires confirmation, Contact e-Dirham System operator for support
3000	Payment failed for normal reasons such as credit card expiry and so on	Requires confirmation, Make sure payment method details are valid
3001	Payment failed insufficient credit.	Requires confirmation
3002	Payment failed card expired	Requires confirmation
4000	You have been black listed, you cannot make payments (Name black list)	Requires confirmation, Contact e-Dirham System operator for support
4001	You have been black listed, you cannot make payments (National Id black list)	Requires confirmation, Contact e-Dirham System operator for support
4002	You have been black listed, you cannot make payments (Bank name black list)	Requires confirmation, Contact e-Dirham System operator for support
4003	You have been black listed, you cannot make payments (Account black list)	Requires confirmation, Contact e-Dirham System operator for support
4004	You have been black listed, you cannot make payments (BIN black list)	Requires confirmation, Contact e-Dirham System operator for support
4005	Card has been rejected.	Requires confirmation, Contact e-Dirham System operator for support
4006	You have been black listed, you cannot make payments (Country black list)	Requires confirmation, Contact e-Dirham System operator for support
4007	You have been black listed, you cannot make payments (IP black list)	Requires confirmation, Contact e-Dirham System operator for support
4100	Transaction e-Dirham System risk rule violation	Requires confirmation, Contact e-Dirham System operator for support
4101	Transaction Merchant risk rule violation	Requires confirmation, Contact e-Dirham System

		operator for support
4103	Transaction Bank risk rule violation	Requires confirmation, Contact e-Dirham System operator for support
2063	2DS authentication failed.	Requires confirmation, Contact e-Dirham System operator for support
2064	Invalid authentication data.	Requires confirmation, Contact e-Dirham System operator for support
2067	Ineligible Card Information.	Requires confirmation, Contact e-Dirham System operator for support
2068	Payment Authentication attempted.	Requires confirmation, Contact e-Dirham System operator for support
2069	Payment Authentication Error.	Requires confirmation, Contact e-Dirham System operator for support
2070	Payment Authentication Failed.	Requires confirmation, Contact e-Dirham System operator for support
2071	Payment Authentication Abnormal Error.	Requires confirmation, Contact e-Dirham System operator for support
2073	Payment Authorization timed out.	Requires confirmation, Contact e-Dirham System operator for support
2074	Payment Authorization invalid response.	Requires confirmation, Contact e-Dirham System operator for support
2075	Response message certificate is invalid.	Requires confirmation, Contact e-Dirham System operator for support
2076	ACS signing certificate expired.	Requires confirmation, Contact e-Dirham System operator for support
2077	Authentication un-available.	Requires confirmation, Contact e-Dirham System operator for support
2082	Invalid Merchant Org Type ID	Requires confirmation,

		Contact e-Dirham System operator for support
2084	3DS Abnormal Error	Requires confirmation, Contact e-Dirham System operator for support
2093	Canceled before submitting card details.	Requires confirmation, Contact e-Dirham System operator for support
2096	Pre-Authorization is not allowed for Non-GII cards.	Requires confirmation, Contact e-Dirham System operator for support
eD-Wallet Error Codes		
WALLET-0000	Payment was processed successfully	Requires confirmation
WALLET-0001	Abnormal error	Contact e-Dirham System operator to support
WALLET-0002	Corrupted eservice data	Send a new request with correct eservice data format
WALLET-0003	Missing Action type	Provide the missing parameter
WALLET-0004	Invalid action type format	Provide valid action type format
WALLET-0005	Missing merchant id	Provide the missing parameter
WALLET-0006	Missing terminal id	Provide the missing parameter
WALLET-0007	Missing Payment unique number	Provide the missing parameter
WALLET-0008	Missing request date	Provide the missing parameter
WALLET-0009	Invalid request date format	Provide valid request date
WALLET-0010	Missing wallet id	Provide the missing parameter
WALLET-0011	Missing eservice data	Provide the missing parameter
WALLET-0012	Invaild eservice data format	Send a new request with correct eservice data format
WALLET-0013	Missing secure hash	Provide the missing parameter
WALLET-0014	Undefined merchant	Contact e-Dirham System operator to support

WALLET-0015	Inactive merchant	Contact e-Dirham System operator to support
WALLET-0016	Deleted merchant	Contact e-Dirham System operator to support
WALLET-0017	Invalid redirect payment merchant URL	Provide valid redirect URL
WALLET-0018	Mismatch secure hash	Contact e-Dirham System operator to support
WALLET-0019	Undefined wallet user	Use defined and active wallet user
WALLET-0020	Inactive wallet user	Use defined and active wallet user
WALLET-0021	Deleted wallet user	Use defined and active wallet user
WALLET-0022	Blocked wallet user	Use defined and active wallet user
WALLET-0023	Undefined default payment method	Use defined and active payment method that selected as default one
WALLET-0024	Inactive default payment method	Use defined and active payment method that selected as default one
WALLET-0025	Deleted default payment method	Use defined and active payment method that selected as default one
WALLET-0026	Inactive wallet	Use active wallet
WALLET-0027	Deleted wallet	Use active wallet
WALLET-0028	Technical error	Contact e-Dirham System operator for support
WALLET-0029	Technical error	Contact e-Dirham System operator for support
WALLET-0030	Technical error	Contact e-Dirham System operator for support
WALLET-0031	Technical error	Contact e-Dirham System operator for support
WALLET-0032	Technical error	Contact e-Dirham System operator for support
WALLET-0033	Technical error	Contact e-Dirham System operator for support
WALLET-0034	Technical error	Contact e-Dirham System operator for support
WALLET-0035	Technical error	Contact e-Dirham System

		operator for support
WALLET-0036	Invalid pass code	Provide valid pass code value
WALLET-0037	User cancel the payment while viewing price	N/A
WALLET-0038	User cancel tha payment before the confirmation	N/A
WALLET-0039	Technical error	Contact e-Dirham System operator for support
WALLET-0040	Technical error	Contact e-Dirham System operator for support
WALLET-0041	Technical error	Contact e-Dirham System operator for support
WALLET-0042	Technical error	Contact e-Dirham System operator for support
WALLET-0043	Technical error	Contact e-Dirham System operator for support
WALLET-0044	Technical error	Contact e-Dirham System operator to support
WALLET-0045	Duplicate Payment unqiue Number	Please change the PUN on each request
WALLET-0046	Missing Token ID	Provide the token id value
WALLET-0047	Missing Reference type	Provide the reference type value
WALLET-0048	Invalid or expired token	Provide a valid token value
WALLET-0050	Reference type value is not valid	Provide the reference type value
WALLET-0051	Invalid token format	Provide a valid token value
WALLET-0052	Secret key is not defined	Please define a secret key through PG access
WALLET-0053	The request JSON format is not valid	Provide a valid JSON format .
WALLET-0055	The request action type is not valid	Provide a valid action type.
WALLET-0056	Invalid Service price value	Provide a valid service price.
WALLET-0057	Invalid service quantity value	provide a valid service quantity value
WALLET-0058	Service quantity missing	provide a valid service quantity value
WALLET-0059	invalid service code format	procide a valid service code value
WALLET-0060	servoce code missing	procide a valid service code value

WALLET-0078	Only G2 Cards are supported for Pre Auth	Provide a G2 Card number
WALLET-0079	Payment Method expired	Provide a valid payment method

Confirm Response Codes

Table 3: Confirm Response Parameters

Status Code	Description	Action to take
EDConnect Error Codes		
EDConnect-0000	Missing "TransactionRequestDate" Parameter	Provide the missing parameter
EDConnect-0006	Missing "MerchantID" Parameter	Provide the missing parameter
EDConnect-0007	Missing "BankID" Parameter	Provide the missing parameter
EDConnect-0023	Merchant is not configured as ED-Connect Merchant	Contact e-Dirham System operator for support
EDConnect-0024	Merchant has no configured secret key	The merchant admin should configure a Secret Key and use it in the Hashing routine
EDConnect-0028	Missing Original transaction "PUN" parameter	Provide to be Auto Updated transaction pun
EDConnect-0029	Missing "SecureHash" parameter	Provide the missing parameter
EDConnect-0030	Secure Hash Could not be validated	Check the parameters used to hash, and recheck the routine in the request parameters
EDConnect-0031	Merchant IP is not supported	Contact e-Dirham System operator for support
EDConnect-0032	Merchant is not available	Send the right merchant ID, or check with e-Dirham System operations team.
EDConnect-0033	Missing "Action" Parameter	Provide the missing parameter
EDConnect-0034	Action type sent is invalid	Provide the right action type for the current request
e-Dirham System Error Codes		
0000	Finished successfully for successful	Do not send any more

	transaction	confirmations for the transaction
1010	An abnormal error occurred	Contact e-Dirham System operator for support
2007	Merchant Id is missing from the merchant's message	Contact e-Dirham System operator for support
2012	Transaction does not exit	Provide a right PUN
2019	OUN is missing from the merchant's message	Contact e-Dirham System operator for support
2079	Merchant's IP is not supported on the payment	Contact e-Dirham System operator for support
2102	Not Payment Router Merchant.	
6501	Merchant is not authorized on e-Dirham System	Contact e-Dirham System operator for support
6502	Merchant ID mismatch	Contact e-Dirham System operator for support
6504	Some or all parameters were missing from the merchant side confirmation message	Contact e-Dirham System operator for support
6506	Merchant's IP is not supported on the payment	Contact e-Dirham System operator for support
6509	Transaction is pending reversal, please try again later	Try again later
6512	Confirmed a failed transaction	Reflect transaction status
6514	Transaction already confirmed	Reflect transaction status
6516	Original transaction is not confirmed	Auto Update the original sale transaction
6517	Transaction status is failed.	Reflect transaction status

Refund Response Codes

Table 4: Refund Response Codes

Status Code	Description	Action to take
EDConnect Error Codes		
EDConnect-0000	Missing "TransactionRequestDate" Parameter	Provide the missing parameter
EDConnect-0001	Missing "TransactionAmount" parameter	Provide the missing parameter
EDConnect-0002	"TransactionAmount" invalid number	Provide the right ISO formatted amount
EDConnect-0003	Missing "Field63_OriginalTransactionUniqueID"parameter	Provide the missing parameter
EDConnect-0004	Missing "Field61_ServiceMainCodeSubCode" parameter	Provide the missing parameter
EDConnect-0005	Missing "Field61_ServiceCodeQuantity" parameter	Provide the missing parameter
EDConnect-0006	Missing "MerchantID" Parameter	Provide the missing parameter
EDConnect-0007	Missing "BankID" Parameter	Provide the missing parameter
EDConnect-0008	Missing "UniqueTransactionID" Parameter	Provide the missing parameter
EDConnect-0009	Missing "TerminalID" Parameter	Provide the missing parameter
EDConnect-0010	Missing "Currency" Parameter	Provide the missing parameter
EDConnect-0011	Missing PoS Entry Mode parameter	Contact e-Dirham System operator for support
EDConnect-0012	PoS Entry Mode Invalid Number	Contact e-Dirham System operator for support
EDConnect-0013	Missing PoS Condition Code parameter	Contact e-Dirham System operator for support
EDConnect-0014	PoS Condition Code Invalid Number	Contact e-Dirham System operator for support
EDConnect-0023	Merchant is not configured as ED-Connect Merchant	Contact e-Dirham System operator for support

EDConnect-0024	Merchant has no configured secret key	The merchant admin should configure a Secret Key and use it in the Hashing routine
EDConnect-0029	Missing "SecureHash" parameter	Provide the missing parameter
EDConnect-0030	Invalid Secure Hash Value	Check the parameters used to hash, and recheck the routine in the request parameters
EDConnect-0031	Merchant IP is not supported	Contact e-Dirham System operator for support
EDConnect-0032	Merchant is not available	Send the right merchant ID, or check with e-Dirham System operations team.
EDConnect-0033	Missing "Action" Parameter	Provide the missing parameter
EDConnect-0034	Action type sent is invalid	Provide the right action type for the current request
e-Dirham System Error Codes		
0000	Refund completed successfully	Transaction is completed successfully, Requires confirmation
0001	Transaction is completed successfully but early auto update failed	Contact e-Dirham System operator for support
9001	Abnormal backend error	Contact e-Dirham System operator for support
1010	An abnormal error occurred	Contact e-Dirham System operator for support
3000	Transaction failed	Requires confirmation , Response received from the backend
2036	Transaction Unique Id already exists	Generate a new Transaction Unique Id for the request
2079	Merchant IP is not supported	Contact e-Dirham System operator for support
2090	Terminal ID mismatch	Contact e-Dirham System

		operator for support
2102	Not Payment Router Merchant.	
5701	Merchant is not authorized to perform refund transaction	Contact e-Dirham System operator for support
5702	Some parameters were missing from the refund request	Add the missing parameters
5703	Transaction has not been marked for refund	Contact your entity's administrator in order to authorize the refund
5704	Transaction has already been refunded	Do not send another refund for this transaction
5706	Refund grace period has been exceeded	Do not send another refund for this transaction
5708	Refund transaction pending Backend error.	Contact e-Dirham System operator for support
5709	Refund transaction Rejected Backend error	Contact e-Dirham System operator for support
5710	The transaction requested to be refunded was not found	Make sure you send a valid transaction Id
5711	An abnormal error occurred	Contact e-Dirham System operator for support
5712	The provided amount was invalid	Send the correct amount value
5713	The unique transaction Id of the refund request has already been used	Generate a new Transaction Unique Id for the request
5714	The unique transaction Id of the refund request has already been used	Send a newer transaction Id
5716	Failed to parse the request message	Contact e-Dirham System operator for support
5717	Request contains no transactions	Contact e-Dirham System operator for support
5718	Unexpected message signature	Contact e-Dirham System operator for support
5719	The transaction is already generated in a voucher	Transaction cannot be refunded

Void Response Codes

Table 5: Void Response Codes

Status Code	Description	Action to take
EDConnect Error Codes		
EDConnect-0000	Missing "TransactionRequestDate" Parameter	Provide the missing parameter
EDConnect-0001	Missing "TransactionAmount" parameter	Provide the missing parameter
EDConnect-0002	"TransactionAmount" invalid number	Provide the right ISO formatted amount
EDConnect-0003	Missing "Field63_OriginalTransactionUniqueID" parameter	Provide the missing parameter
EDConnect-0006	Missing "Merchant" ID Parameter	Provide the missing parameter
EDConnect-0007	Missing "BankID" Parameter	Provide the missing parameter
EDConnect-0008	Missing "UniqueTransactionID" Parameter	Provide the missing parameter
EDConnect-0009	Missing "TerminalID" Parameter	Provide the missing parameter
EDConnect-0010	Missing "Currency" Parameter	Provide the missing parameter
EDConnect-0011	Missing PoS Entry Mode parameter	Contact e-Dirham System operator for support
EDConnect-0012	PoS Entry Mode Invalid Number	Contact e-Dirham System operator for support
EDConnect-0013	Missing PoS Condition Code parameter	Contact e-Dirham System operator for support
EDConnect-0014	PoS Condition Code Invalid Number	Contact e-Dirham System operator for support
EDConnect-0023	Merchant is not configured as ED-Connect Merchant	Contact e-Dirham System operator for support
EDConnect-0024	Merchant has no configured secret key	The merchant admin should configure a Secret Key and use it in the Hashing routine
EDConnect-0029	Missing "SecureHash" parameter	Provide the missing

		parameter
EDConnect-0030	Secure Hash Could not be validated	Check the parameters used to hash, and recheck the routine in the request parameters
EDConnect-0031	Merchant IP is not supported	Contact e-Dirham System operator for support
EDConnect-0032	Merchant is not available	Send the right merchant ID, or check with e-Dirham System operations team.
EDConnect-0033	Missing "Action" Parameter	Provide the missing parameter
EDConnect-0034	Action type sent is invalid	Provide the right action type for the current request
e-Dirham System Error Codes		
0000	Void was successful	Requires confirmation
9001	Abnormal backend error	Contact e-Dirham System operator for support
1010	An abnormal error occurred	Contact e-Dirham System operator for support
3000	Transaction failed	Requires confirmation , Response received from the backend
2079	Merchant IP is not supported	Contact e-Dirham System operator for support
2090	Terminal ID mismatch	Contact e-Dirham System operator for support
2102	Not Payment Router Merchant.	
5601	Some parameters were missing from the void request	Add the missing parameters
5602	Merchant is not authorized to perform void transaction	Contact e-Dirham System operator for support
5603	Transaction has already been voided	Do not send another void for this transaction
5605	Exceeded void grace period	Do not send another void for this transaction as the transaction cannot be voided
5608	An error occurred while parsing the request message	Contact e-Dirham System operator for support
5611	Transaction not marked for void	Contact your entity's

		administrator to flag the transaction for void
5612	Void Transaction failed backend error.	Contact e-Dirham System operator for support
5613	Void Transaction Timed out backend error.	Contact e-Dirham System operator for support
5614	Void Transaction Not found backend error.	Contact e-Dirham System operator for support
5615	Invalid void amount received	Send the right amount to be voided
5616	transaction is already generated in a voucher	Transaction cannot be voided

E-Service inquiry Response Codes

Table 6: E-Service Inquiry Response Codes

Status Code	Description	Action to take
EDConnect Error Codes		
EDConnect-0000	Missing "TransactionRequestDate" Parameter	Provide the missing parameter
EDConnect-0006	Missing "Merchant" ID Parameter	Provide the missing parameter
EDConnect-0007	Missing "BankID" Parameter	Provide the missing parameter
EDConnect-0008	Missing "UniqueTransactionID" Parameter	Provide the missing parameter
EDConnect-0009	Missing "TerminalID" Parameter	Provide the missing parameter
EDConnect-0010	Missing "Currency" Parameter	Provide the missing parameter
EDConnect-0011	Missing PoS Entry Mode parameter	Contact e-Dirham System operator for support
EDConnect-0012	PoS Entry Mode Invalid Number	Contact e-Dirham System operator for support
EDConnect-0013	Missing PoS Condition Code parameter	Contact e-Dirham System operator for support
EDConnect-0014	PoS Condition Code Invalid Number	Contact e-Dirham System operator for support
EDConnect-0015	Missing "ApplicationNumber" Parameter	Provide the missing parameter
EDConnect-0017	Missing "EServiceMainCodeSubCode_*" Parameter	Provide the missing parameter
EDConnect-0018	Missing "EServiceQuantity_*" Parameter	Provide the missing parameter
EDConnect-0019	"EServiceQuantity_*" Invalid Number	Provide the right numeric value
EDConnect-0020	Missing "PaymentMethodType" Parameter	Provide the missing parameter
EDConnect-0021	PaymentMethodType invalid format	Provide the right format (X-X)
EDConnect-0022	"EServiceMainCodeSubCode_*" invalid	Provide the right MainCode-

	format	SubCode format (XXXXXX-XXXX)
EDConnect-0023	Merchant is not configured as ED-Connect Merchant	Contact e-Dirham System operator for support
EDConnect-0024	Merchant has no configured secret key	The merchant admin should configure a Secret Key and use it in the Hashing routine
EDConnect-0029	Missing "SecureHash" parameter	Provide the missing parameter
EDConnect-0030	Secure Hash Could not be validated	Check the parameters used to hash, and recheck the routine in the request parameters
EDConnect-0031	Merchant IP is not supported	Contact e-Dirham System operator for support
EDConnect-0032	Merchant is not available	Send the right merchant ID, or check with e-Dirham System operations team.
EDConnect-0033	Missing "Action" Parameter	Provide the missing parameter
EDConnect-0034	Action type sent is invalid	Provide the right action type for the current request
e-Dirham System Error Codes		
0000	Eservice Inquiry Completed Successfully	-
2010	Currency not supported by merchant	Contact e-Dirham System operator for support
2036	Transaction Unique Id already exists	Generate a new Transaction Unique Id for the request
2079	Merchant IP is not supported	Contact e-Dirham System operator for support
2085	Transaction Unique Id already exists	Generate a new Transaction Unique Id for the request
2088	Requested Eservice does not exist on e-Dirham System	Contact e-Dirham System operator for support
2089	Duplicate Eservice code sent in request	Send only unique e-Serivces in request
2090	Terminal ID mismatch	Contact e-Dirham System operator for support
2092	Payment method is not supported by merchant	Contact e-Dirham System operator for support

2102	Not Payment Router Merchant.	
3003	Invalid intended action received	Please send Payment or Authorize as the intended action
5801	The max different eservices exceeded in request	Contact e-Dirham System operator for support
5802	The max quantity of eservices exceeded in request	Contact e-Dirham System operator for support
5803	The eservice is not assigned to merchant	Contact e-Dirham System operator for support
5807	Missing request parameters	Contact e-Dirham System operator for support
5808	Not able to authenticate merchant	Contact e-Dirham System operator for support
5809	The requested eservice is ZERO amount eservice	Provide the eservice amount in the request
5810	The e-service is not assigned to merchant in e-Dirham service management	Contact e-Dirham System operator for support
6150	Inactive eservice owner	Contact e-Dirham System operator for support
6151	Inactive eservice	Contact e-Dirham System operator for support
6152	Inactive e-Dirham service	Contact e-Dirham System operator for support
2083	Inactive merchant	Contact e-Dirham System operator for support
2004	Merchant is not available	Contact e-Dirham System operator for support

Completion Response Codes

Table 7: Completion Response Codes

Status Code	Description	Action to take
EDConnect Error Codes		
EDConnect-0000	Missing “TransactionRequestDate” Parameter	Provide the missing parameter
EDConnect-0001	Missing “TransactionAmount” parameter	Provide the missing parameter

EDConnect-0002	"TransactionAmount" invalid number	Provide the right ISO formatted amount
EDConnect-0025	Missing "Field61_InqTrxnID" parameter	Provide the missing parameter
EDConnect-0026	Missing "Field61_InqAuthCode" parameter	Provide the missing parameter
EDConnect-0027	Missing "Field61_InqRRN" parameter	Provide the missing parameter
EDConnect-0006	Missing "Merchant" ID Parameter	Provide the missing parameter
EDConnect-0007	Missing "BankID" Parameter	Provide the missing parameter
EDConnect-0008	Missing "UniqueTransactionID" Parameter	Provide the missing parameter
EDConnect-0009	Missing "TerminalID" Parameter	Provide the missing parameter
EDConnect-0010	Missing "Currency" Parameter	Provide the missing parameter
EDConnect-0011	Missing PoS Entry Mode parameter	Contact e-Dirham System operator for support
EDConnect-0012	PoS Entry Mode Invalid Number	Contact e-Dirham System operator for support
EDConnect-0013	Missing PoS Condition Code parameter	Contact e-Dirham System operator for support
EDConnect-0014	PoS Condition Code Invalid Number	Contact e-Dirham System operator for support
EDConnect-0023	Merchant is not configured as ED-Connect Merchant	Contact e-Dirham System operator for support
EDConnect-0024	Merchant has no configured secret key	The merchant admin should configure a Secret Key and use it in the Hashing routine
EDConnect-0029	Missing "SecureHash" parameter	Provide the missing parameter
EDConnect-0030	Secure Hash Could not be validated	Check the parameters used to hash, and recheck the routine in the request parameters
EDConnect-0031	Merchant IP is not supported	Contact e-Dirham System operator for support
EDConnect-0032	Merchant is not available	Send the right merchant ID, or check with e-Dirham

		System operations team.
EDConnect-0033	Missing “Action” Parameter	Provide the missing parameter
EDConnect-0034	Action type sent is invalid	Provide the right action type for the current request
e-Dirham System Error Codes		
0000	Completion transaction completed successfully	Requires Confirmation
0001	Transaction is completed successfully but early auto update failed	Contact e-Dirham System operator for support
1010	Abnormal error	Contact e-Dirham System operator for support
2010	Currency not supported by merchant	Contact e-Dirham System operator for support
2036	Transaction Unique Id already exists	Generate a new Transaction Unique Id for the request
2046	Request timed out Backend Error	Contact e-Dirham System operator for support
2079	Merchant IP address is not supported	Contact e-Dirham System operator for support
2086	Merchant parameter is not authorized	Contact e-Dirham System operator for support
2087	Merchant parameter is missing	Contact e-Dirham System operator for support
2090	Terminal ID mismatch	Contact e-Dirham System operator for support
2102	Not Payment Router Merchant.	
5511	Completion already performed on provided PUN	Don’t send another request
5512	Pre-Authorization transaction reversed	Contact e-Dirham System operator for support
5502	Pre-Authorization transaction does not exist	Pre-Authorization must be sent first
5508	Completion amount does not match blocked amount (pre authorize amount)	Send the right amount for completion
5509	Currency does not match Pre-Authorization currency	Send the right currency for completion
5510	Pre-Authorization transaction is voided	Don’t send another request
6152	Inactive e-Dirham Service	Contact e-Dirham System operator for support

eD-Wallet Error Codes		
WALLET-0000	Payment was processed successfully	Requires confirmation
WALLET-0001	Abnormal error	Contact e-Dirham System operator to support
WALLET-0002	Corrupted eservice data	Send a new request with correct eservice data format
WALLET-0003	Missing Action type	Provide the missing parameter
WALLET-0004	Invalid action type format	Provide valid action type format
WALLET-0005	Missing merchant id	Provide the missing parameter
WALLET-0006	Missing terminal id	Provide the missing parameter
WALLET-0007	Missing Payment unique number	Provide the missing parameter
WALLET-0008	Missing request date	Provide the missing parameter
WALLET-0009	Invalid request date format	Provide valid request date
WALLET-0010	Missing wallet id	Provide the missing parameter
WALLET-0011	Missing eservice data	Provide the missing parameter
WALLET-0012	Invaild eservice data format	Send a new request with correct eservice data format
WALLET-0013	Missing secure hash	Provide the missing parameter
WALLET-0014	Undefined merchant	Contact e-Dirham System operator to support
WALLET-0015	Inactive merchant	Contact e-Dirham System operator to support
WALLET-0016	Deleted merchant	Contact e-Dirham System operator to support
WALLET-0017	Invalid redirect payment merchant URL	Provide valid redirect URL
WALLET-0018	Mismatch secure hash	Contact e-Dirham System operator to support
WALLET-0019	Undefined wallet user	Use defined and active wallet user
WALLET-0020	Inactive wallet user	Use defined and active wallet

		user
WALLET-0021	Deleted wallet user	Use defined and active wallet user
WALLET-0022	Blocked wallet user	Use defined and active wallet user
WALLET-0023	Undefined default payment method	Use defined and active payment method that selected as default one
WALLET-0024	Inactive default payment method	Use defined and active payment method that selected as default one
WALLET-0025	Deleted default payment method	Use defined and active payment method that selected as default one
WALLET-0026	Inactive wallet	Use active wallet
WALLET-0027	Deleted wallet	Use active wallet
WALLET-0028	Technical error	Contact e-Dirham System operator for support
WALLET-0029	Technical error	Contact e-Dirham System operator for support
WALLET-0030	Technical error	Contact e-Dirham System operator for support
WALLET-0031	Technical error	Contact e-Dirham System operator for support
WALLET-0032	Technical error	Contact e-Dirham System operator for support
WALLET-0033	Technical error	Contact e-Dirham System operator for support
WALLET-0034	Technical error	Contact e-Dirham System operator for support
WALLET-0035	Technical error	Contact e-Dirham System operator for support
WALLET-0036	Invalid pass code	Provide valid pass code value
WALLET-0037	User cancel tha payment while viewing price	N/A
WALLET-0038	User cancel tha payment before the confirmation	N/A
WALLET-0039	Technical error	Contact e-Dirham System operator for support
WALLET-0040	Technical error	Contact e-Dirham System operator for support
WALLET-0041	Technical error	Contact e-Dirham System

		operator for support
WALLET-0042	Technical error	Contact e-Dirham System operator for support
WALLET-0043	Technical error	Contact e-Dirham System operator for support
WALLET-0044	Technical error	Contact e-Dirham System operator to support
WALLET-0045	Duplicate Payment unqiue Number	Please change the PUN on each request
WALLET-0046	Missing Token ID	Provide the token id value
WALLET-0047	Missing Reference type	Provide the reference type value
WALLET-0048	Invalid or expired token	Provide a valid token value
WALLET-0050	Reference type value is not valid	Provide the reference type value
WALLET-0051	Invalid token format	Provide a valid token value
WALLET-0052	Secret key is not defined	Please define a secret key through PG access
WALLET-0053	The request JSON format is not valid	Provide a valid JSON format .
WALLET-0055	The request action type is not valid	Provide a valid action type.
WALLET-0056	Invalid Service price value	Provide a valid service price.
WALLET-0057	Invalid service quantity value	provide a valid service quantity value
WALLET-0058	Service quantity missing	provide a valid service quantity value
WALLET-0059	invalid service code format	procide a valid service code value
WALLET-0060	servoce code missing	procide a valid service code value
WALLET-0078	Only G2 Cards are supported for Pre Auth	Provide a G2 Card number
WALLET-0079	Payment Method expired	Provide a valid payment method

length Error Codes		
EDConnect	8000	**Bank id invalid length**
EDConnect	8001	Currency code invalid length
EDConnect	8002	Terminal id invalid length
EDConnect	8003	Unique transaction id invalid length
EDConnect	8004	Transaction request date invalid length
EDConnect	8005	Transaction amount invalid length
EDConnect	8006	Service inquiry auth code invalid length
EDConnect	8007	Service inquiry rrn invalid length
EDConnect	8008	Service inquiry trxn id invalid length
EDConnect	8009	Action parameter invalid length
EDConnect	8010	Merchant id invalid length
EDConnect	8011	Secure hash invalid length
EDConnect	8012	Original transaction unique id invalid length
EDConnect	8013	Eservice service code sub code invalid length
EDConnect	8014	Eservice quantity invalid length
EDConnect	8015	Original PUN invalid length
EDConnect	8016	Card expiry date invalid length
EDConnect	8017	Card holder name invalid length
EDConnect	8018	Card number invalid length
EDConnect	8019	CSC invalid length
EDConnect	8020	Payment method invalid length
EDConnect	8021	National id invalid length
EDConnect	8022	Language invalid length
EDConnect	8023	Payment Description invalid length
EDConnect	8024	Merchant Module SessionID

		invalid length
EDConnect	8025	Application number invalid length
EDConnect	8026	Intended e-Dirham Service invalid length
EDConnect	8027	Version invalid length
EDConnect	8028	Eservice price invalid length
EDConnect	8029	Eservice quantity invalid length
EDConnect	8030	Eservice service code sub code invalid length
EDConnect	8031	Merchant response URL invalid length

Appendix C: Generate Message Secure Hash

The secure hash is generated from the preconfigured merchant's secrete key and some request/response parameters using HMAC-SHA256 algorithm.
The merchant can generate the secure hash by following the below steps:

- Prepare the data that used to generate the secure hash, as mentioned for each action
- Use SHA-256 algorithm to generate the secure hash
- The result of Secure Hash must be Base64 encoded

Actions

Table 8: Action values

Action Value	Action Description
28	e-Service Inquiry
0	Pay-Web
32	Pre-Auth
33	Completion
30	Void
37	Refund
13	Auto Update

Appendix D: Encrypt Card Holder Info

The merchant must use "Password Based Encryption" method to encrypt the card holder information, then the cipher results must be Base64 encoded.

The card holder inof consist of

- Card expiry date
- Card holder name
- Card number
- CVV2

The below steps must be followed to handle each card holder info before send it:

- Use the "**AES 128 Bit, CBC Block Cipher Mode**" as encryption algorithm, the algorithm needs key and Intialization Vector to prform encryption process.
- The encryption key is actualy the hashed merchant's sercret key using SHA-256 with empty salt.
- The Intialization Vector is the first 16 bytes of the hashed merchant's secret key.
- Perform the encryption process.
- Finally the result must be Base64 encoded.

Appendix E: Merchant Admin - Secret Key Configuration

This section describes the steps necessary for Merchant Administrator to configure/set the Secret Key needed to integrate with Payment Router.

Pre-Conditions:

- Merchant Admin is logged in.
- Merchant Admin has the privilege to Manage e-Dirham services ("Update ED-Connect Secret Key")

Flow:

- Merchant Admin selects "Update ED-Connect Secret Key"
- Merchant Admin is requested to re-enter his authentication password as in Figure 3 below.

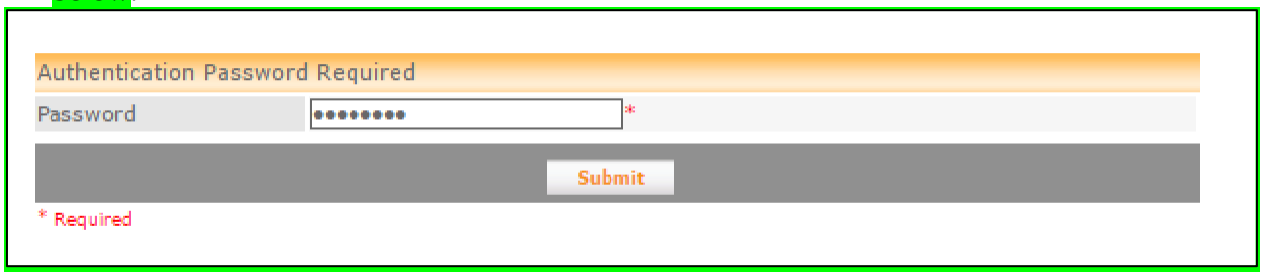

Figure 3 - Authentication Page

- System displays the "Edit ED-Connect Secret Key Screen" with the current configured Secret Key as in figure 4 below.

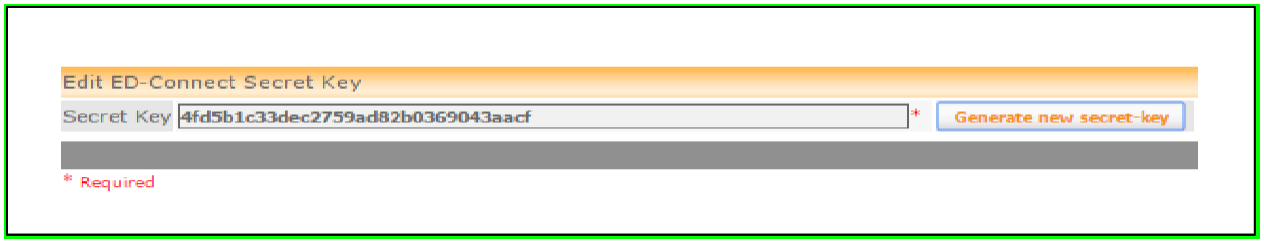

Figure 4 - Merchant secret key screen

- Merchant Admin clicks on the "Generate new secret-key".
- Pop up message appears to confirm the update.
- System generates a new Secret Key value and saves it encrypted in the database.

Appendix F: Security recommendations in handling the secret key

The following recommendations could be advised for storing the Secret Key securely:

- Use Java KeyStore or .NET Data Protection API to protect the secret key. The KeyStore password could be stored in the configuration files.
- Use File System permissions to restrict access to the application configuration files. Application admins must ensure that configuration files are not web accessible in any way.
- Use strong integrity checks on the application JARS/WARS/DLLS/etc to make sure that they are not modified during runtime.
- Use extensive logging to observe the usage of the secret key and use alerts for any suspicious behavior