Technical Specification Document (Fonepay Web Integration)

Version 2.0

September 2020

Contents

Document Control

Document Name	Technical Specification Document - Fonepay WEB Integration
Document number	
Document Owner	

Document Version	Date	Created/Modified By	Reviewed By	Approved By	Remarks / Amendments

Introduction

This document contains the standard specifications of the interface between the merchant site (your website) and merchant convergent application. The interface specification describes at a technical level the communication of data between the merchant's site and the merchant convergent application. Data exchanged between the merchant's site and the merchant convergent system that does not strictly match the format specified in this document is rejected.

Payment Integration Specifications

Payment System consists of two steps:

1. Request Payment

Payment need to be initiated by redirecting to fonepay system by providing parameters as well as

return URL (RU) to receive response from fonepay system.

2. Verify Payment Response

Merchant site needs to check and verify payment response of fonepay. To verify response, merchant should check Data Validation (DV)
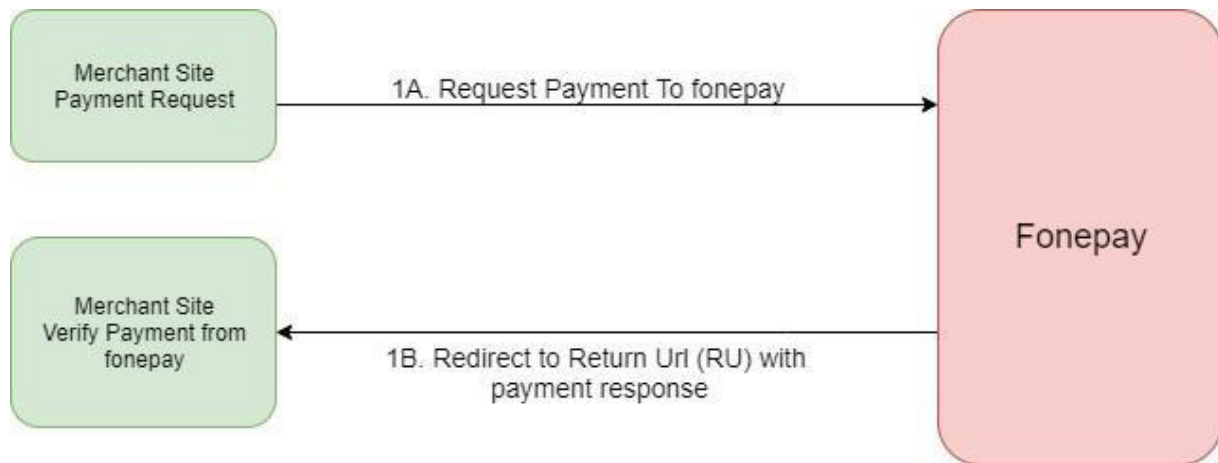
Parameter Details for Payment Request:

All parameters are mandatory.

Query Param	Datatype	Length	Description
RU	String	Max 150	Return URL where Fonepay system notifies payment information to merchant site
PID	String	Min 3 Max 20	Merchant Code, Defined by fonepay system
PRN	String	Min 3 Max 25	Product Reference Number, need to send by merchant
AMT	Double	Max 18	Payable Amount
CRN	String	Fixed 3	Default Value, NPR need to send for local merchants

		Fixed 10	Format: MM/DD/YYYY eg:06/27/2018
DT	String		
R1	String	Max 160	Need to provide payment details that identifies what was payment for (E.g. Receipt id or payment description)
R2	String	Max 50	Additional Info, provide N/A if does not exists
MD	String	Min 1 Max 3	P –payment
DV	String		SHA512 hashed value. Read Secure Hash Calculation (DV) below to generate this value

Secure Hash Calculation (DV)

The SHA-512 HMAC HEX is calculated as follows:

1. All transaction fields are concatenated with value of each field string with ',' after every field except the last field.

Order to concat:

PID,MD,PRN,AMT,CRN,DT,R1,R2,RU

(value should not be URL encoded when generating Data Validation).

2. The above string is then hashed using HMAC with UTF-8 encoded Shared Secret as key.

3. The generated hash is then converted into hexadecimal.

For example, if the Shared Secret is a7e3512f5032480a83137793cb2021dc, and the transaction request includes the following fields:

https://dev-clientapi.fonepay.com/ape/merchantRequest?PID=NBQM&MD=P&AMT=30&CRN=NPR&DT=06%2F27%2F2017&R1=Hello&R2=test+remarks&DV=099d8532de44b4b1387d3cfe74408a8c801d6551ba6b7b437846670ecd6145f618de55169fbdae1b0cb5104c64e79b60483f7ef0f7bd22b57a7fa83c9fcf9cf0&RU=https%3A%2F%2Fdev-adminapi.fonepay.com%2FConvergentMerchantDummyweb%2FMerchantVerification&PRN=d1580724437729

Note: Key for HMAC_SHA512 will be provided by fonepay system.key will be different for test & production System. Do not share Secret Key with others and do not store where others may easily find them like front-end website, app and merchant should generate HMAC_SHA512 in backend and store Secret Key in secure location.

Example of a Secure Hash Calculation

NBQM,P,d1580724437729,30,NPR,06/27/2017,Hello,test remarks,
https://devadminapi.fonepay.com/ConvergentMerchantDummyweb/MerchantVerification

Calculated Hash
(DV) 099d8532de44b4b1387d3cfe74408a8c801d6551ba6b7b437846670ecd6145f618de55169fbdae1b0cb5104c64e79b60483f7ef0f7bd22b57a7fa83c9fcf9cf0

Implementation

Fonepay System URL:

- Dev Server(For Testing): https://dev-clientapi.fonepay.com
- Live Server: https://clientapi.fonepay.com

1. Payment Implementation

Merchant need to send request fonepay system by redirecting to foneapay payment URL with all parameters defined. Fonepay system will redirect with transaction details to URL provided in RU parameter by merchant site while initiating payment.

A. Request Payment to Fonepay

Merchants need to send a GET or a POST request with the following details:

(Note: Please make sure HTTP GET Request is URL encoded if you are using GET request)

Example:

While Testing with Fonepay test server

https://dev-clientapi.fonepay.com/api/merchantRequest?PID=NBQM&MD=P&AMT=30&CRN=NPR&DT=06%2F27%2F2017&R1=Hello&R2=test+remarks&DV=099d8532de44b4b1387d3cfe74408a8c801d6551ba6b7b437846670ecd6145f618de55169fbdae1b0cb5104c64e79b60483f7ef0f7bd22b57a7fa83c9fcf9cf0&RU=https%3A%2F%2Fdev-adminapi.fonepay.com%2FConvergentMerchantDummyweb%2FMerchantVerification&PRN=d1580724437729

When using production use

Live Server: https://clientapi.fonepay.com

B. Response from fonepay

After payment by customer Fonepay System redirects to return URL with transaction details and payment status.

https://dev-adminapi.fonepay.com/ConvergentMerchantDummyweb/MerchantVerification?PRN=d1580724437729&PID=NBQM&PS=true&RC=successful=667860224021DF1891F7DE873A37B1DEDA720CCDC43F6

3BC88F86ED20F579E0DE66526D37C71B1D14A8D466E4B740D17D4FF274CD2819FD6ED2AA3D9A89D7C52&UID=36463&BC=NICENPKA&INI=9841845631&P_AMT=20.0&R_AMT=30

Details of Received Response Parameter:

Parameter Details for Payment Response:

Parameters	Description
PRN	Same value provided by Merchant during payment request
PID	Merchant Code
PS	Payment Status true if payment is success and false if payment failed
RC	Transaction Response Code which defines payment state as successful, failed, cancel
DV	Data Validation, merchant needs to verify if DV value calculated by merchant is same as value provided by fonepay in URL
UID	Fonepay Trace Id (Trace ID), should be maintained by merchants which will be user while reconciling transactions.
BC	Bank Swift Code from where user has made payment or esewa if payment is done from esewa. Value may be "N/A" in case of failed case.
INI	Initiator user made payment .Value may be "N/A" if value is not available.

P_AMT	Paid total amount by customer, it can be different from R_AMT as fonepay charges/discount may include. In above example: Amount of Rs 30.0 was request by merchant in step 1A for payment and if Rs 10.0 is discount by fonepay system then transaction P_AMT is 20.0 In case of a failed case amt may be same as requested amount in Step 1A.
R_AMT	Amount Requested by merchant

Merchant needs to verify if DV value calculated by merchant is the same as value provided by fonepay in URL.

To generate DV check following example:

Secure Hash Calculation (DV)

PRN,PID,PS,RC,UID,BC,INI,P_AMT,R_AMT

Example of a SecureHash Calculation
d1580724437729,NBQM,true,successful,36463,NICENPKA,9841845631,20.0,30

Hash (DV) =

667860224021DF1891F7DE873A37B1DEDA720CCDC43F63BC88F86ED20F5
79E0DE66526D37C71B1D14A8D466E4B740D17D4FF274CD2819FD6ED2AA
3D9A89D7C52

https://dev-adminapi.fonepay.com/ConvergentMerchantDummyweb/MerchantVerification?PRN=d1580724437729&PID=NBQM&PS=true&RC=successful=667860224021DF1891F7DE873A37B1DEDA720CCDC43F63BC88F86ED20F579E0DE66526D37C71B1D14A8D466E4B740D17D4FF274CD2819FD6ED2AA3D9A89D7C52&UID=36463&BC=NICENPKA&INI=9841845631&P_AMT=20.0&R_AMT=30

2. Check Transaction Status

Introduction

It is a standard specification of the interface between the merchant System and Fonepay System to check transaction status. This interface specification describes a technical level communication of data between the merchant System and the Fonepay System. Data exchanged between merchant and Fonepay system that does not strictly match the format specified in this document is rejected

Implementation

Fonepay System URL:

Dev Serve(For Testing): https://dev-merchantapi.fonepay.com/api

Live Serve: https://merchantapi.fonepay.com/api

Verification Request

Merchant need to send request from merchant System to Fonepay system.

Merchant need to send POST request with following details:

Example:

https://FonepaySystemURL/api/merchant/merchantDetailsForThirdParty/txnVerification

Replace Fonepay System URL with Dev Serve (For Testing)

https://dev-merchantapi.fonepay.com/convergent-merchantweb/api/merchant/merchantDetailsForThirdParty/txnVerification

OR Replace Fonepay System URL with Live Serve

https://merchantapi.fonepay.com/api/merchant/merchantDetailsForThirdParty/txnVerification

NOTE:

Authorization:

To Generate Authorization header value, Username and password are combined into a string "username: password" the resulting string is then encoded using Base64 encoding. The authorization method and a space i.e. "Basic " is then set before the encoded string.

For example, if the user agent uses **'gnw71090@zwoho.com'** as the username and **'Fonepay@12345**' as the password then the header is formed as follows:

Authorization: Basic Z253NzEwOTBAendvaG8uY29tOkZvbmVwYYXlAMTIzNDU=

NOTE:

Username	Username of merchant panel provided by Fonepay
password	Password of Merchant panel provided by Fonepay

auth

To Generate **auth** header value, generate HMAC_SHA512 with Key for HMAC_SHA512

Secret Key = Secret Key provide in your merchant profile page after you login.

Message for HMAC_SHA512=> accessUser,accessPassword,method,

contentType,resource,JSON _Request Replace Param above with actual value.

Note: Value is separated by comma and value should not be URL encoded.

For Example:

Key => a7e3512f5032480a83137793cb2021dc

=> Message

gnw71090@zwoho.com,Fonepay@12345,POST,application/json,/merchant/merchantDetailsFor
ThirdParty/txnVerification,{"prn": "d1549791827186","merchantCode": "NBQM","amount":
"30"} So our hash for auth header is as follow:

**0d3ebe65246182596de0d417e8e39d37ebe2f5da028c52ae0a33a05062a3bded8a737
c3ff82b6f1a6d9442d11cfcb0432d86998af81f481948c0af7b346f4fa2**

Transaction Verification Request

Field Name	Format	Length	Condition	Description
prn	AN	Max = 50	Mandatory	UniqueId provide by merchant
merchantCode	AN	1-15	Mandatory	Merchant Code provided by fonepay system
amount	N	1-10	mandatory	The value shall only include (numeric) digits "0" to "9" and may contain a single "." character as the decimal mark. When the amount includes decimals, the "." character shall be used to separate the decimals from the integer value.

#. JSON Message Sample

Json format that merchant system should generate while sending transaction verification request and the response generated by the fonepay system is as follow:

Request URL	https://dev-merchantapi.fonepay.com/convergent-merchant-web/api/merchant/merchantDetailsForThirdParty/txnVerification
METHOD	POST

Header	**Content-Type:** application/json Authorization: Basic Z253NzEwOTBAendvaG8uY29tOkZvbmVwYXllAMTIzNDU= **auth**: 0d3ebe65246182596de0d417e8e39d37ebe2f5da028c52ae0a33a05062a3bded8a737c3ff82b6f1a6d9442d11cfcb0432d86998af81f481948c0af7b346f4fa2
Request	{"prn": "d1549791827186","merchantCode": "NBQM","amount": "30"}

Success Response	{
	  "clientCode": "",
	  "fonepayTraceId": 12847,
	  "initiator": "",
	  "merchantCode": "NBQM",
	  "paymentStatus": "pending",
	  "prn": "d1549791827186",
	  "requestedAmount": "30",
	  "totalTransactionAmount": "",
	  "transactionDate": "2019-02-10T15:28:54+05:45",
	  "transactionType": ""
	}

	Authentication Failure Response:
	<code>{</code>
	"documentation": "User not Authorized",
	"errorCode": 401,
	"message": "cannot access this resource"
	}
	VALIDATION Failure Response:
	[
	{
	"fieldType": "merchantCode",
	"message": "merchant code cannot be empty"
	}
	]
Failure Response	

Sample Project And Code:

1. Sample Java Spring Boot Project:

https://github.com/fonepay/Fonepay-Spring-Boot-Integration-Sample

2. Sample code to Generate HMAC (Java) public String generateHash(String secretKey,

   String message) {

Mac sha512_HMAC = null;

String result = null; try { byte[] byteKey = secretKey.getBytes("UTF-8"); final

String

HMAC_SHA512 = "HmacSHA512"; sha512_HMAC

= Mac.getInstance(HMAC_SHA512);

SecretKeySpec keySpec = new SecretKeySpec(byteKey, HMAC_SHA512);

sha512_HMAC.init(keySpec);   result   =

bytesToHex(sha512_HMAC.doFinal(message.getBytes("UTF-8")));

return result; } catch (Exception e) { log.error("Exception while

Hashing Using HMAC256");

return null;

} } private static String bytesToHex(byte[] bytes) { final char[]

hexArray = "0123456789ABCDEF".toCharArray(); char[]

hexChars = new char[bytes.length * 2];

for (int j = 0; j < bytes.length; j++) { int v =

bytes[j] & 0xFF; hexChars[j * 2] =

hexArray[v >>> 4]; hexChars[j * 2 + 1] = hexArray[v

& 0x0F];

}   return   new

String(hexChars);

}

3. PHP SAMPLE CODE FOR PAYMENT AND VERIFY PROCESS

For Payment

```php
<?php


$autoSubmission = true;


$MD = 'P';

$AMT = '10';

$CRN = 'NPR';

$DT = date('m/d/Y');

$R1 = 'test';

$R2 = 'test';

$RU = 'http://localhost/verify.php'; //fully valid verification page link

$PRN = uniqid();


$PID = 'NBQM';

$sharedSecretKey = 'a7e3512f5032480a83137793cb2021dc';
```

```php
$DV = hash_hmac('sha512',
$PID.','.$MD.','.$PRN.','.$AMT.','.$CRN.','.$DT.','.$R1.','.$R2.','.$RU, $sharedSecretKey);


$paymentLiveUrl = 'https://clientapi.fonepay.com/api/merchantRequest';

$paymentDevUrl = 'https://dev-clientapi.fonepay.com/api/merchantRequest';

?>
```

```html
<!DOCTYPE html>

<html>

<head>

<title>Fonepay Payment page</title>

</head>

<body>

<form method="GET" id ="payment-form" action="<?php echo $paymentDevUrl; ?>">

<input type="hidden" name="PID" value="<?php echo $PID; ?>" >

<input type="hidden" name="MD"    value="<?php echo $MD; ?>">

<input type="hidden" name="AMT" value="<?php echo $AMT; ?>">

<input type="hidden" name="CRN" value="<?php echo $CRN; ?>">

<input type="hidden" name="DT" value="<?php echo $DT; ?>">

<input type="hidden" name="R1" value="<?php echo $R1; ?>">

<input type="hidden" name="R2" value="<?php echo $R2; ?>">

<input type="hidden" name="DV" value="<?php echo $DV; ?>">

<input type="hidden" name="RU" value="<?php echo $RU; ?>">

<input type="hidden" name="PRN" value="<?php echo $PRN; ?>">
```

```html
<input type="submit" value="Click to Pay">

</form>


</body>

</html>


<?php if ($autoSubmission ==

true): ?> <script>    window.onload=function(){ window.setTimeout(function() {

document.getElementById("payment-form").submit(); }, 2500);

};

</script>

<?php endif; ?>
```