Technical Specification Document (Fonepay Web Integration)

Version 2.0

September 2020

Contents

Document Control 1

Introduction 2

Payment Integration Specifications 2

1. Request Payment 2

2. Verify Payment Response 2

Parameter Details For Payment Request: 3

Implementation 5

1. Payment Implementation 5

A. Request Payment To Fonepay 6

B. Response from Fonepay 6

Parameter Details for Payment Response 7
Sample Project And Code: 9

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:

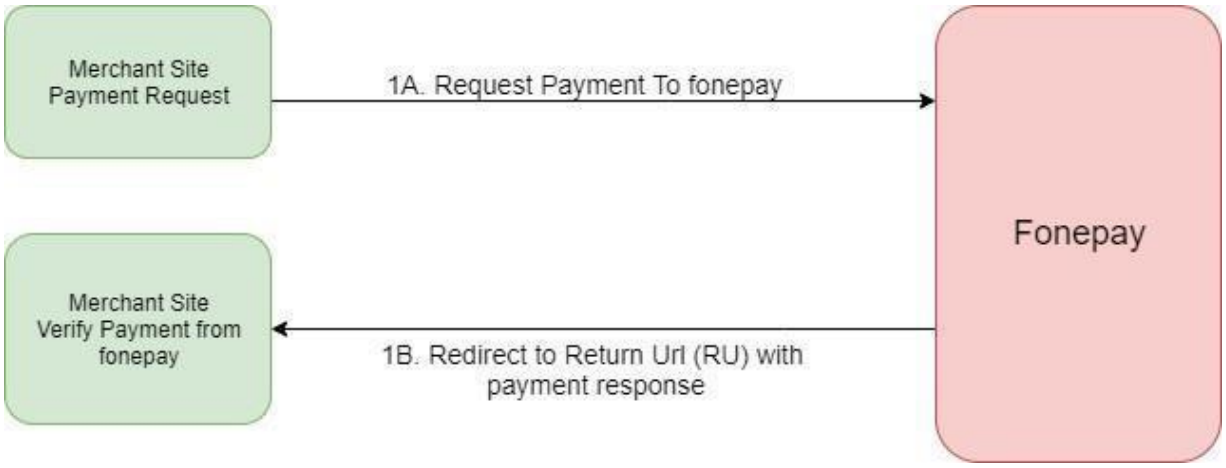
1. **Request Payment**

Payment need to be initiated by redirecting to the Fonepay system by providing parameters as

well as a return URL (RU) to receive a response from the Fonepay system.

2. **Verify Payment Response**

   The merchant site needs to check and verify the payment response of Fonepay. To verify the response,the 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, needs to send by the merchant
AMT	Double	Max 18	Payable Amount
CRN	String	Fixed 3	Default Value, NPR needs to send for local merchants

DT	String	Fixed 10	Format: MM/DD/YYYY eg:06/27/2017
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 exist
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 the 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 **fonepay**, and
the transaction request includes the following fields:

https://dev-clientapi.fonepay.com/api/merchantRequest?PID=fonepay123&MD=P&AMT=30&CRN=NPR&DT=06%2F27%2F2017&R1=Hello&R2=test&DV=099d8532de44b4b1387d3cfe74408a8c801d6551ba6b7b437846670ecd6145f618de55169fbdae1b0cb5104c64e79b60483f7ef0f7bd22b57a7fa83c9fcf9cf0&RU=https%3A%2F%2Fdev-adminapi.fonepay.com%2FConvergentMerchantDummyweb%2FMerchantVerification&PRN=d1580724437729

Note: The key for HMAC_SHA512 will be provided by Fonepay system. key will be different for test & production Systems. 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

fonepay123,P,d1580724437729,30,NPR,06/27/2017,Hello,test,
https://devadminapi.fonepay.com/ConvergentMerchantDummyweb/MerchantVerification

Calculated Hash
(DV)147384cc250bf072fdacbce811da683a3ed7f5f7d1c0dd2ce2fb90d27d69b2bc3c143306aa4fa26625a171ac0d4d2e2aaa53e4e10902eb9418eac32f591b92c0

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 Fonepay 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=fonepay123&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=fonepay123&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,fonepay123,true,successful,36463,NICENPKA,9841845631,20.0,30

Hash (DV) =

667860224021DF1891F7DE873A37B1DEDA720CCDC43F63BC88F86ED20F579E0DE66526D37C71B1D14A8D466E4B740D17D4FF274CD2819FD6ED2AA3D9A89D7C52

https://dev-adminapi.fonepay.com/ConvergentMerchantDummyweb/MerchantVerification?PRN=d1580724437729&PID=fonepay123&PS=true&RC=successful=667860224021DF1891F7DE873A37B1DEDA720CCDC43F63BC88F86ED20F579E0DE66526D37C71B1D14A8D466E4B740D17D4FF274CD2819FD6ED2AA3D9A89D7C52&UID=36463&BC=NICENPKA&INI=9841845631&P_AMT=20.0&R_AMT=3

Sample Code:

1. 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);
}
```

2. PHP SAMPLE CODE FOR PAYMENT AND VERIFY PROCESS

For Payment

```
<?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 = 'fonepay123';
$sharedSecretKey = 'fonepay';
```

```
$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';

?>

<!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; ?>">
```

```
<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; ?>
```