

Circular: NPCI/2018-19/RuPay/009

14th May, 2018

To All Member Banks – RuPay

Dear Sir/Madam,

Subject - Changes in RuPay eCommerce specifications regarding hashing (Important Implementation)

Overview

Due to recent fraud transactions using RuPay Cards on eCommerce platform, RBI had released an advisory to introduce hashing in PaySecure specifications. We have made the necessary changes to the PaySecure specification and require the changes to be implemented at Issuer and Acquirer banks end.

Background

Recently, we had come across incidents of possible Man-in-the-Middle (MITM) during the time of OTP validation for eCommerce transactions using RuPay cards. The response codes sent from Issuer Authentication Server (IAS) (due to their visibility in plain text in the payment gateway browser page) was tampered and subsequently transmitted to PaySecure platform. PaySecure does a second level of validation of auth_result API call where in the IAS system is requested to verify the result. NPCI was getting success response in both level which had resulted in initiation of authorisation request by PaySecure to the customers' banks.

RBI has released an advisory # 2/2018 dated 16th April 2018 wherein banks are advised to ensure that encryption/secure hashing mechanism is put in place in the communication/data exchange between IAS and PaySecure system, through browser or any other mode. The same has to be implemented by 31st July 2018.

Implementation Details

From Issuer perspective the following changes have to be implemented –

- The Auth_Initiate API call is used for checking card details as provided by Cardholder. PaySecure will securely pass the card details including card number, expiry date, CVD2 and Transaction ID (unique value generated by PaySecure) along with a Hash Key (hkey) to the issuer in this call.
- Dynamic HKEY will be used by IAS to validate the hash code received from Acquirer in OTP Page re-direction request.
- The same key will be required to generate the hash code for the authentication response to be sent to Acquirer.
- During Cardholder interaction, a new parameter is introduced named as AccuRequestId which will be used to avoid tampering of request data in transit, the issuer is required to provide a hash code

Page 1 of 2

for the acquirer to validate. This hash code can be generated by hashing AccuGuid, session, AccuResponseCode and Transaction ID parameter value.

- If the hash messages do not match, the IAS is required to decline transaction and give response code ACCU600.

From Acquirer perspective the following changes have to be implemented –

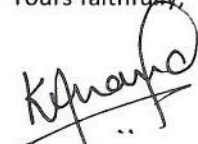
- PaySecure will provide a TransactionID, AccuGUID, HKEY & RedirectURL in “Initiate2” response back to Acquirer, to which the URL of cardholder needs to be redirected to initiate authentication process.
- Acquirer will be generate hash code by hashing AccuCardholderId, AccuGuid, session and Transaction ID parameter value and final hash value will be pass in the redirection request parameter name as AccuRequestId.
- Once authentication is completed by Issuer IAS, the acquirer will be generate hashvalue using AccuGuid, session, AccuResponseCode ,Transaction ID and Key(HKEY) then match the output value generate by acquirer against the AccuRequestId value received in authentication response sent by Issuer IAS.If the hash value do not match, the acquirer is required to decline transaction and do not proceed further with authorization request to NPCI.

All hash code generation and validation should be done at bank’s server level using HMAC_SHA256 algorithm.

Acquirer & Issuers are strongly recommended not to pass/use/communicate secrete Hash Key i.e. hkey in any way over browser communication or to any third party. Acquirer & Issuers are liable to manage the secrecy of Hash Key i.e. hkey at their respective environment/infrastructure.

All Member Banks are requested to kindly take a note of the aforesaid. For any queries, you may please contact Neelesh Gupta at 7506446579 or write at neesh.gupta@npci.org.in

Yours faithfully,



Vishal Anand Kanvaty
SVP – Innovation & Product