National Payment Corporation of India

Guidelines for

“Hashing”

Contents

1. Introduction

In lieu with the recent events, NPCI has decided to make certain changes in the RuPay eCommerce system which should improve the overall customer experience and reduce instances of fraud. These changes are additional to the URL redirection migration which is currently in progress. These additional activities include Hashing (mandated by RBI), inclusion of amount and merchant name during authentication leg and User agent compliance by NPCI according to NPCI guidelines.

2. Hashing

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 debit 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.

In URL redirection flow, during OTP validation for RuPay eCommerce the communications takes place between Acquirer and Issuer using customer browser which is vulnerable to man in the middle attack. To reduce this threat it is advised to implement hashing mechanism, whereby banks and its vendors will be advised to ensure that encryption/secure hashing mechanism is put in place in the communication/data exchange, through browser or any other mode. Hashing of the value will be done using a common key available only to the acquirer and the issuer involved.

3. Amount and Merchant Name

Currently for RuPay eCommerce, the transaction amount and merchant name is not shared with Bank or bank's ACS vendor during Authentication leg Many banks have requested us to share the transaction amount and merchant name during the time of authentication; so that they can display the same on the OTP page opened for the cardholder or send these details with OTP message to the cardholder during authentication.

As part of the current eCommerce flow, PaySecure makes auth initiate API call to IAS vendor/Issuer Bank to check the availability of cardholder's mobile details. PaySecure share the following details (parameters) in this call –

1. user id
2. password
3. Tran_id
4. cardholder status
5. card details (card number, expiry,CVD2)

6. language code
7. version

But transaction during auth initiate call, amount and merchant name is not shared with the IAS vendor/issuer banks. NPCI has decided that during Auth_inititate API, PaySecure should send the auth _amount and terminal_owner_name, so that bank can share the same with their cardholders during online transaction. This should improve the overall cardholder experience and reduce the chances of fraud transaction.

4. Guidelines

Development is required at both issuer and acquirer end for the above mentioned activities. Please make note of the following points -

- During certification for these activities the test transaction has to be fired by bank or bank's vendor. Screenshot and logs also has to be shared by the bank or bank's vendor with NPCI.

- Banks which have already completed or are in process of certification of URL redirection will continue with their existing plan. Subsequently such banks will have to certify for hashing before 31 July 2018.

- Two round (Comfort and UAT) of testing has to be done for these activities.

- For issuer or acquirer who are not certified or migrated to URL redirection will have to do the certification for the same with hashing.

4.1.1 Issuer Development

Issuer Bank has to make development at their IAS/ACS level for the following activities –

- **Hashing**

1. 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.
2. Dynamic HKEY will be used by IAS to validate the hash code received from Acquirer in OTP Page re-direction request.
3. The same key will be required to generate the hash code for the authenticaiton response to be sent to Acquirer.
4. 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 for the acquirer to validate. This hash code can be generated by hashing AccuGuid, session, AccuResponseCode and Transaction ID parameter value.

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

- **Amount and Merchant Name** – PaySecure will share the amount and merchant name with bank's IAS/ACS system. Bank should be able to utilise these details to display these details to cardholders the merchant and amount name on OTP page and also send these details to cardholders in the OTP number message (SMS). Specification for these changes will be released in 10 – 15 days.

4.1.2 Acquirer Development

Acquirer has to make development at their end for the following activities –

- **Hashing**

1. 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.
2. 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.
3. 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.
4. Hash key will be passed to acquirer in RedirectURL parameter in Initiate2 response.

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.

5. Timelines

RBI has mandated that all the banks should have implemented hashing by 31st July 2018.

END OF DOCUMENT