NPCI/2024-25/NACH/005 November 18,2024

To,

All NACH member banks,

Corporates & Aggregators participating in NACH.

Implementation of AES Encryption in ONMAGS Application

To enhance the data security and ensuring compliance with modern encryption standards, we are implementing the Advanced Encryption Standard (AES) as the mandatory encryption protocol within the ONMAGS Application for all authentication modes. The technical specifications are provided in Annexure I.

The banks and corporates that are ready with the new encryption mode can approach NPCI to get certified to move to production. All the members are advised to move to the new encryption methodology before January 31, 2025. It may please be noted that this is related to security related change we will not extend the timelines any further. Non – compliance will lead to action that may lead to discontinuation of the services to the participants that are non-compliant.

The information herein may please be disseminated to all the concerned for compliance, queries may be routed through CRM.

With warm regards,

SD
Giridhar G.M.
Chief-Customer Success

ONMAGS AES-GCM ENCRYPTION
TSD

1.0

Contents

1 Introduction

ONMAGS receives the mandate creation request from the merchants and the same is passed to the destination bank .Data flowing in the request and response are signed,encrypted and encoded from the sender and the receiver has to decrypt ,verify the signature and decode to get the plain request and vice versa .Also checksum is generated for each request/response which is sent along when data is passed between sender and receiver.This is done to enhance the security of the data flowing as part of the request/response .

2 Overview of the existing process

- Currently parties involved in the mandate request are generating the checksum with the defined logic .
- Data flowing in the request is individually encrypted and placed in the request XML tags using RSA encryption.
- For this purpose ,NPCI is using the bank public key certificate given by the bank.
- Once the encryption is done,NPCI will sign the request using NPCI private key certificate.
- The encrypted signed request is further encoded to prevent any malicious attack and sent to destination bank along with checksum .
- Destination bank has to decode ,decrypt and then verify the signature and process the actual request.

3 Proposed process flow

- In order to enhance further security ,it is proposed to use AES-GCM encryption which is symmetric encryption which encrypts using 256 bit key .
- AES -GCM provides faster way to encrypt the data and also it can handle large amount of data in lesser time when compared to RSA encryption.

4 Details of the encryption process

- This change is applicable only for the newly onboarded merchants and the banks .
- There will be an option given in the admin portal for the participant to opt for the new encryption approach.
- This option is provided in the participant master where they can select to opt for AES encryption .
- If AES encryption is selected ,then the merchants are expected to encrypt the entire payload with the AES-GCM encryption and then sign and encode the request as per existing process and send the same to ONMAGS.
- There is no change in the checksum logic while sending the request .
- ONMAGS will decode ,verify the signature and decrypt the request using AES-GCM encryption .
- Then ONMAGS will process the request and then use the same encryption AES-GCM approach to send the request to the destination bank.
- Destination banks has to use the same approach to decrypt and process the mandate request .
- Merchants,banks and ONMAGS will be using AES-GCM with No padding version for this implementation .Session/secret Key length would be 8 digit.

5 Detailed flow of the encryption process for Merchants

- Merchants should generate the session key /secret key for every request with AES-GCM with no padding version.
- Existing logic to be used for check sum generation.
- Merchants has to encrypt the entire payload request using the session key/secret key .
- Then they have to encrypt the check sum value using the session/secret key .
- Once the payload and the check sum are encrypted ,then they have to use NPCI public key to encrypt the session key using RSA algorithm as per the existing process.
- Once the session key is encrypted,then the merchants should sign the request using their private key.
- After signing the request ,they have to encode the request as per existing process using URL encoding.
- After encoding the request ,they have to send to NPCI .
- Merchants will follow the same procedure (as mentioned in the flow diagram 5.3.2) while receiving the request from NPCI.

5.1 Detailed flow of the decryption process for NPCI

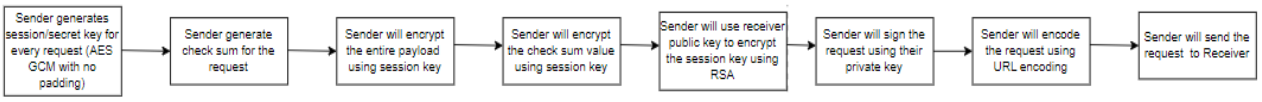
- Once NPCI receives the request ,NPCI will decode the request using existing process.
- After decoding the request ,NPCI will verify the signature using merchant public key.
- NPCI will use their private key to decrypt the session key from the request using the RSA approach which is used currently.
- Then NPCI will use the session key to decrypt the actual payload sent by the merchants.
- Once the payload is decrypted,then NPCI will decrypt the check sum using the session key.
- Once the check sum is decrypted,NPCI will validate the check sum sent in the request .
- Once the check sum validation is succesful,NPCI will process the request.
- NPCI will follow the same procedure (as mentioned in the flow diagram 5.3.1) while sending the request to destination banks .

5.2 Detailed flow of the decryption process for banks

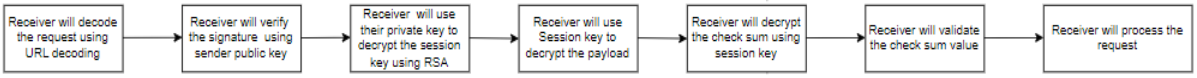
- Once banks receives the request ,banks will decode the request using existing process.
- After decoding the request ,banks will verify the signature using NPCI public key.
- Banks will use their private key to decrypt the session key from the request using the RSA approach which is used currently.
- Then banks will use the session key to decrypt the actual payload sent by NPCI.
- Once the payload is decrypted,then banks will decrypt the check sum using the session key.
- Once the check sum is decrypted,banks will validate the check sum sent in the request.
- Once the check sum validation is succesful,banks will process the request.
- Banks will follow the same procedure (as mentioned in the flow diagram 5.3.1) while sending the request to NPCI.

5.3 Flow diagram of the AES-GCM

5.3.1 Request sent from sender to receiver



5.3.2 Request processing at receiver



6 Summary View of End to End approach

Merchant to ONMAGS				
Request Flow	**Encrypt**	**Sign**	**Verify the signature**	**Decrypt**
Merchant to ONMAGS	1.Merchant to use Session key to encrypt payload. 2.Merchant will use NPCI Public key to encrypt the session key sent in the request.	Merchant will sign using their private key	ONMAGS will verify the signature using Merchant public key	1.ONMAGS will use NPCI private key to decrypt the session key. 2.Then use session key to decrypt the payload.
ONMAGS to Merchant	1.ONMAGS will use Session key to encrypt payload. 2.ONMAGS will use Merchant public key to encrypt the session key.	ONMAGS will sign using NPCI private key	Merchant will verify the signature using NPCI public key	1.Merchant will use their Private key to decrypt the session key. 2.Then use session key to decrypt the payload.
ONMAGS to bank				
Request Flow	**Encrypt**	**Sign**	**Verify the signature**	**Decrypt**
ONMAGS to bank	1.ONMAGS will use session key to encrypt the payload.	ONMAGS will sign using NPCI private key	Banks will verify the signature using NPCI public key	1.Banks will use their Private key to decrypt the session key.

	2.ONMAGS will use Bank Public key to encrypt the session key.			2.Then use session key to decrypt the payload.
Bank to ONMAGS	1.Banks will use Session key to encrypt payload request. 2.Bank will use NPCI public key to encrypt the session key.	Bank will sign the request using Private key	ONMAGS will verify the signature using Bank public key	1.ONMAGS will Use NPCI Private key to decrypt the session key. 2.Then Use session key to decrypt the payload.
****Different keys will be used for encryption and signing by Merchant /NPCI/banks**				

7 Assumptions

- NPCI,banks and merchants will have two different set of keys for encrypting and signing the request .
- Code logic for the AES-GCM approach will be shared by NPCI to merchants and banks and they have to use the same for decrypting the request.

End of Document