NPCI
भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

NPCI/2019-20/CTS/037

January 21, 2020

To,

All CTS Member banks

Introduction of Advance Encryption Standard (AES)

Currently DES (Digital Encrypted Standard) is used for data transmission between banks and NPCI, for better security and other enhanced benefits it has been decided to implement Advanced Encryption Standard (AES) at CCH. The primary features of AES are

1. Symmetric key block cipher
2. Quick response compared to DES
3. 128 bit data & 256 bit keys

The updated version of DEM specification version 8.0 is enclosed to this circular.

The summary of changes is provided below:

Sl. No	Details	Page number	Version Number
1	Added changes for AES Encryption/Decryption algorithms.	23-28	8.0

In order to facilitate smooth transition CCH is equipped with capability to handle DES as well as AES encryption in parallel therefore there is no impact on the banks. The member banks are advised to take note of the facility and migrate to AES before February 28, 2020. Member banks implementing DEM form now on should implement AES only.

CHI banks can continue to use the current DES encryption logic and separate communication will be issued for AES migration.

Note that from March 01, 2020 CCH will stop accepting data encrypted using DES. All the member banks should strictly adhere to the timelines.

With warm regards,

Giridhar G M
Chief-Offline product operations & technology