NATIONAL PAYMENTS CORPORATION OF INDIA

NACH Project

Bank Specification Document

Version 3.1

March, 2015

DOCUMENT RELEASE NOTICE

Document Details

Name	Version No.	Date	Description
Bank Specifications Document	1.0	20th July 2012	Provides operations and technical details that bank needs to be ready with for on-boarding of ACH platform.
Bank Specifications Document	1.1	28th August 2012	Updated section 3.4 Digital file signing
Bank Specifications Document	1.2	12th November 2012	Updated section 3.2 for Records per text file Added Section 3.6 for Checksum Updated section 4 to include updated file formats, sample files and Error Codes
Bank Specifications Document	1.4	28th December 2012	Updated sec 4 to include updated file formats for NACH. Also added XML file formats
Bank Specifications Document	1.6	26thMar 2013	Updated mapper file format based on existing one used in production Added details for Aadhaar Lookup (UID Status) File
Bank Specifications Document	2.1	19th July 2013	Modified sample files
Bank Specifications Document	2.2	28th October 2013	Added Success flags for RES files and APBS mapper. Added PKCS#7 Signing in Section 3.8

Bank Specifications Document	2.3	24th December 2013	Inclusion of Checksum Validations in section 3.6 Addition of following content: - Bulk file upload - Bank Extension - Mark pending Changes in Existing APBS Product
Bank Specifications Document	2.4	17th January 2014	Inclusion of UID RES File format and sample files
Bank Specification Document	2.7	30th June 2014	Time zone +5:30 was include for all pain format's ISODate and ISODateTime fields.
	3.0	16th September 2014	1. Note added regarding file name extension (Section 2.2) 2. Note regarding the usage of flag and reason code (Section 2.2) 3. Bank Extension & Mark Pending: More details included (Section 2.2) 4. A new subsection included regarding validation of files without session and DEL file generation (Section 2.2) 5. APBS Process section updated (Section 2.4) 6. Note added regarding reason codes maintained in NACH front end (Section 4) 7. Registration document updated.
	3.1	11th February 2015	Added AV file description and Mapper file description. Appendix 7 - Added AV File formats and sample file. Appendix 8 - Added New Mapper formats and sample file.

This document and any revised pages are subject to document control. Please keep them up-to-date using the release notices from the distributor of the document.

Table of Contents

1. INTRODUCTION 5

2. INTERFACE SPECIFICATION DETAILS FOR NPCI ACH 6

2.1 REGISTRATION WITH NPCI 6

2.2 ACH PROCESS 6

2.3 MMS PROCESS ..... **ERROR! BOOKMARK NOT DEFINED.**

2.4 APBS PROCESS 13

3. HARDWARE AND SYSTEM SOFTWARE 16

3.1 DESKTOP 16

3.2 FILE SIZE AND RECORD SIZE 16

3.3 DIGITAL CERTIFICATES 17

3.4 DIGITAL FILE SIGNING ..... **ERROR! BOOKMARK NOT DEFINED.**

3.5 ACH FILE SIGNING USING PKCS#7 SIGNATURE IN JAVA 17

3.6 NETWORK BANDWIDTH 18

3.7 LOGIC FOR CHECKSUM 18

3.8 VERHOEFF ALGORITHM 19

4. APPENDIX 20

APPENDIX 1 – NACH FILE FORMATS 20

APPENDIX 2 – MMS FILE FORMATS ..... **ERROR! BOOKMARK NOT DEFINED.**

APPENDIX 3 – SAMPLE FILES 20

APPENDIX 4 – REGISTRATION DOCUMENTS ..... **ERROR! BOOKMARK NOT DEFINED.**

APPENDIX 5 – REASON CODES FOR ACH AND MANDATE FILES ..... **ERROR! BOOKMARK NOT DEFINED.**

APPENDIX 6 – ISO ERROR CODES FOR ACH FILE VALIDATIONS ..... **ERROR! BOOKMARK NOT DEFINED.**

APPENDIX 7 – AV FILE DESCRIPTION, FILE FORMATS AND SAMPLE FILE 21

APPENDIX 8 – NEW MAPPER FORMATS AND SAMPLE FILE 22

1. Introduction

This document details the requirement of banks to use the NPCI NACH system. The document talks about the requirements for using the system, and also the different file formats for payment transactions. It also provides the return reason codes to be provided by Banks as part of the Return file.

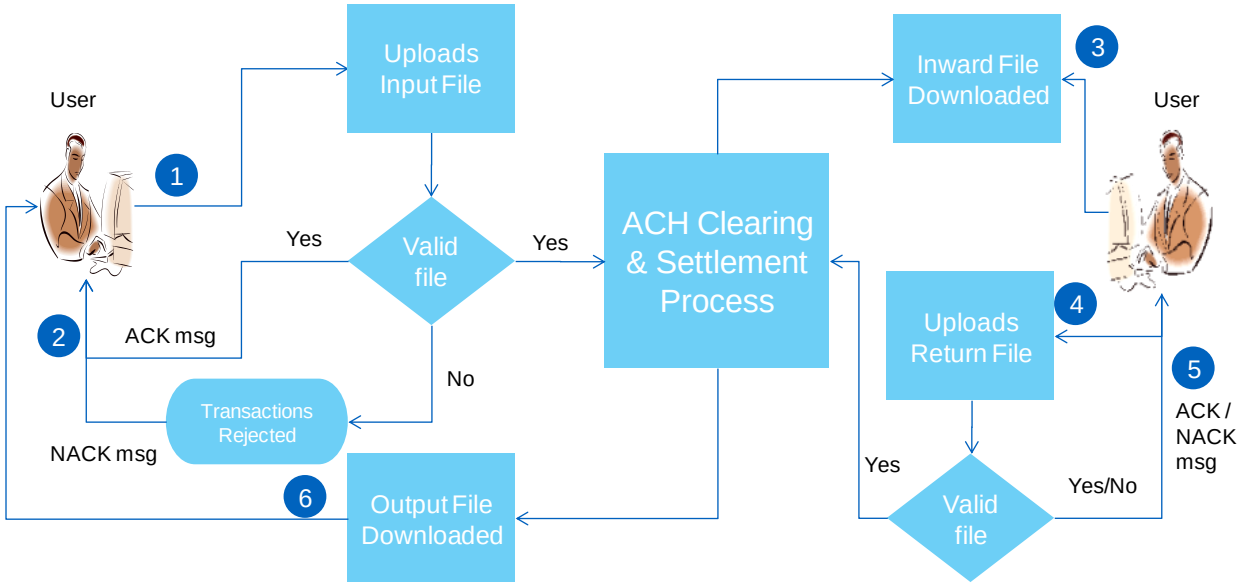
2. Interface specification details for NPCI ACH

2.1 Registration with NPCI

- Submit necessary documents as per the NPCI guidelines provided in Appendix 4 – Registration Documents
- NPCI reviews the document and creates the Participant in the ACH system
- After participant creation, NPCI will create Admin user and/or Bank user for bank
- Login ID should be minimum of 4 characters in length. First four characters should be corporate or bank identifier. This is for clarity purpose only, however not for system validation.

2.2 ACH Process

Following is the ACH process that will be followed. This paragraph explains the type of files that the Bank needs to send and receive from ACH solution.



The numbers depict the sequential flow of the files for every Input File sent across by the initiating bank.

File 1 – Sponsor Bank User submits/uploads the file for a product (using the Upload / Download option in the left hand pane after logging into NACH application). The file will be authorized by the Sponsor Bank checker through the Front End (under Routing -> Files -> Approve).

Note:

1. Files uploaded by the bank through Host-to-Host or SFTP file transfer, will not require Bank checker approval. This is applicable for files uploaded by either Sponsor or Destination Bank.

File 2 – System generates an acknowledgement file for the file submitted into ACH system. For file uploaded by DCA, Sponsor Bank & DCA will receive the acknowledgement file.

File 3 – System generates inward file to Destination Bank for the transactions settled during the presentation session.

File 4 – Destination Bank User needs to submit the Return file for the Inward transactions. Once the file is uploaded, the authorizing or returning will be through front end screen. The file will need to be approved by the Destination Bank Checker User.

File 5 - System generates an acknowledgement file for the return file uploaded into NACH

File 6 – System generates final output file (response file) to the Sponsor Bank for the Input file submitted. For Input File uploaded by DCA, Sponsor & DCA will receive the Response File (RES).

The format and process will be common for ACH Credit, ACH Debit, CECS Credit, APB Credit and EBT Credit files.

Other File Types

File 7: APBS Mapper File

This file is used for mapping an Aadhaar Number to a bank (identified by an IIN i.e. Institution Identification Number, a 6 digit numeric identifier generated by NPCI). This will be stored in the repository and will be checked while processing ACH (APB) and APBS transaction files.

File 8: VLookup File

Bank will have the option to check whether an Aadhaar number is in the UID repository and is in status active or not. Bank user will upload a file having list of Aadhaar numbers which he or she wants to check for status. System will generate a Response file containing the status for each record provided in the input file.

The reason codes for various validations are provided in Appendix 5 – Reason Codes for ACH and Mandate Files.

NOTE: The files that are sent from upload/download screen to the application (ACH, MMS) have to be given a format of txt, xml or csv in the lower case. If .TXT, .XML or .CSV is given in upper case then SFG will throw an error and the file will not reach ACH.

File 7: APBS Mapper File Format

For the updation of UID Mapper Database, APBS Mapper file will be used to identify the bank (through IIN code; a 6 digit numeric identifier issued by NPCI) for a particular Aadhaar number. This mapper file will update the details in the database, and when APBS files with Aadhaar number are submitted, the system will search for this Aadhaar number in the repository and then based on the IIN, the transaction will be routed to the respective destination bank.

File Naming Convention

<ProcessName>-<TransType>-<Bank Identifier>-<LoginId>-<Date>-<nnnnnn>-**MAP**.txt

E.g. ACH-CM-HDFC-HDFC001-07062012-000001-**MAP**.txt

Status codes and description

Status Code	Remarks
0	Mandate date in the record must be greater than that of the existing UID
1	Duplicate UID record
2	Future Mandate Date is not accepted
3	Fresh insert must be Active only
5	Aadhaar Number is not mapped to your IIN or Scheme
7	Inserted For the First Time
8	Updated UID record
9	Invalid Aadhaar_No, Verhoeff Checksum validation Failed
10	Invalid Aadhaar_No, Aadhaar number is not equal to 12 digits
11	Invalid Aadhaar_No, Aadhaar Number must not start with 1

File Format

The file format is provided in Appendix 1 - NACH File Formats.

File 8: Aadhaar Lookup (UID Status) File

Bank will have the option to check whether an Aadhaar number is in the UID repository and is in active status or not. Bank user will upload a file having list of Aadhaar numbers for which status has to be checked. System will generate a Response file containing the status for each record provided in the input file.

Input File Naming convention

<ProcessName>-<TransType>-<Bank Identifier>-<LoginId>-<Date>-<nnnnnn>-INP.txt

- Process Name –UID
- Trans Type –ST
- Bank Identifier – 4 Char Unique Bank Identifier in System

- LoginId - User Login Id
- Date – ddmmyyyy (Date of Upload)
- nnnnnn – 6 digit running sequence number

E.g. UID-ST-SBIN-SBINUser01-22032013-000001-INP.txt

Output File Naming convention

<ProcessName>-<TransType>-<Bank Identifier>-<LoginId>-<Date>-<nnnnnn>-RES.txt

E.g. UID-ST-SBIN-SBINUser01-22032013-000001-RES.txt

File Format

File formats are as follows

Input File

Sr. No	Field Description	Length	Field Type	Mandatory /Optional	Remarks
1	Aadhaar Number	12	NUM	M	Aadhaar number to be checked for status from database

Output File

Sr. No	Field Description	Length	Field Type	Mandatory /Optional	Remarks
1	Aadhaar Number	12	NUM	M	Aadhaar number provided in Input file
2	Status	1	NUM	M	Status from Database, values will be 0/1/2/3

The output file will have "|" as a delimiter between Aadhaar Number and the corresponding status fields.

Status codes and description

Status Code	Remarks
0	Aadhaar Number is in Status Active
1	Aadhaar Number is in Status Inactive
2	Aadhaar Number is Not Present in Database
3	Not a Valid Aadhaar Number

Success Flags in Response Files

Note: The flag value along with the reason code should be used for determining the actual status of the transaction.

Success Flags in Response files for various status

Success Flag	Remarks
0	Success Flag for Returned transaction
1	Success Flag for Accepted transaction
2	Success Flag for Rejected transaction
3	Success Flag for Mark Pending/Bank Extension transaction
4	Success Flag for transactions not processed. This will happen in the case where you send two different product type records in ACH, and each has a different session. So, in one session the transaction will process for one product type, and in the other it will process the other product type. The RES will mention in the first file with 4 for those not yet run. In the second RES, it will be changed accordingly
5	Success Flag for transaction Recall
6	Success Flag for unwound transaction
7	Success Flag for Deemed Accepted transaction

Bulk File Upload:

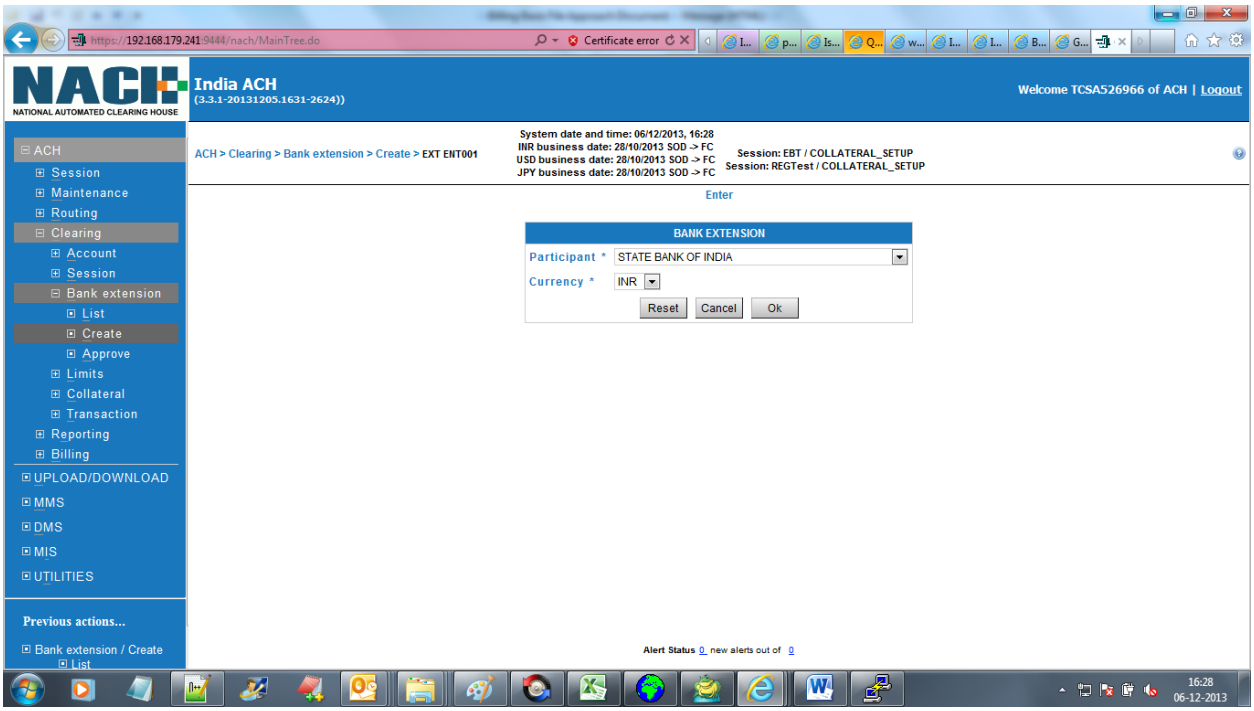
Bulk file upload is done through SFG in which we can define certain limit for the number of transactions that will be present in the Input file. According to the maximum limit set, the Input file will get split into certain number of Bulk files, each having the limit as the number of transactions. These files come into ACH and get processed and eventually there is equal number of Response files that gets generated. These response files are sent to SFG and are combined to form one single response file. However, the SFG user gets both the Single response as well as the bulk response files.

Bank Extension & Mark Pending:

Bank Extension:

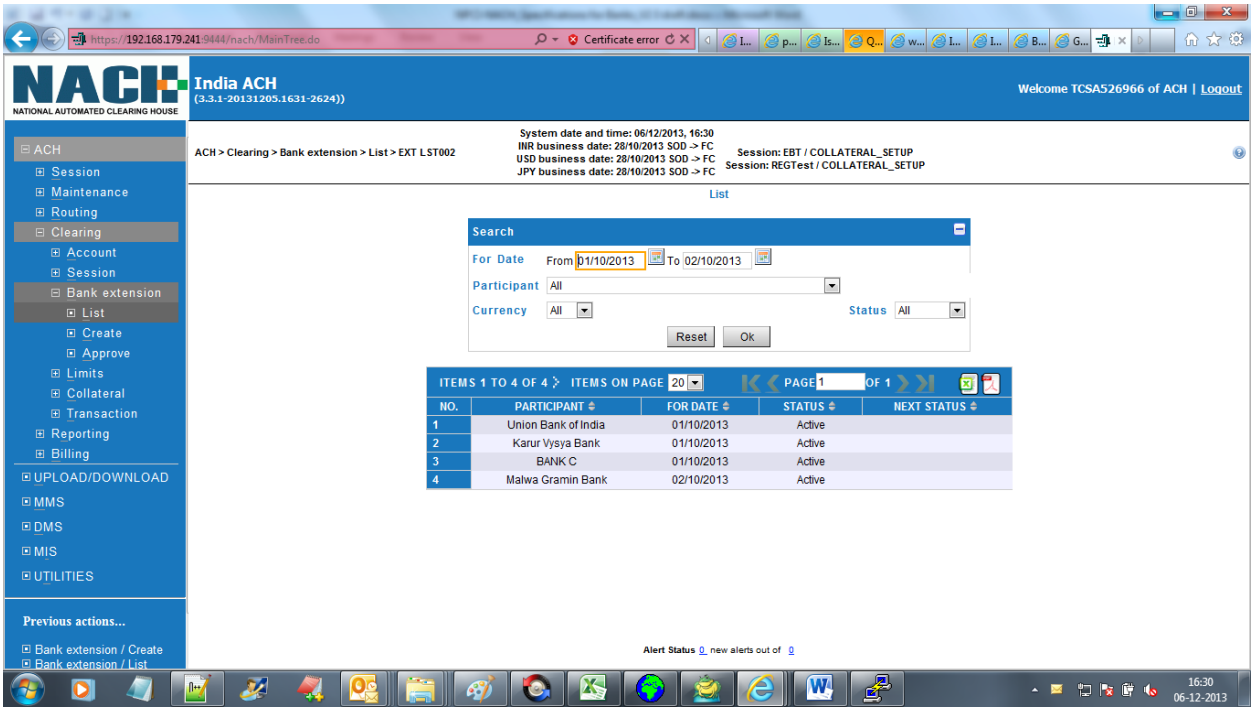
Bank Extension is an extension of certain amount of business days given to some destination Bank participants who needs time to make a decision on whether to Return some transactions or let them get

deemed accepted. After doing a Bank Extension and on clearing the return session all the transactions for the Bank which was extended will automatically get marked pending. If a user wants certain transactions to be extended, certain others to be returned and some to be deemed accepted then he can send a return file with Return reason codes or deemed acceptance codes for some transactions. All the other Transactions will be marked as Pending. Bank Extension is done by NPCI.



Here the NPCI Admin will define for which participant & currency he is doing a Bank Extension. After the user has done create, the same has to be approved.

After approval the NPCI Admin user can view for which participants he has done a bank extension by going to List view



Bank Extension is done preferably after ending the presentation session and before starting the return session. Bank Extension can be done bank wise only i.e. this will be applicable across all products and open sessions.

The Number of days by which the bank will be extended is defined in the back end in a file called module.xml. Currently, bank extension can be given to a bank for a day by NPCI. This will grant one day extension, and the bank can upload the return file on the next business day. On the first day, the response file received by the Sponsor Bank, will have the normal file naming convention (as discussed in File 6 under ACH Process). This response file will have the transactions pertaining to the destination bank (for which the extension was given), as pending (Flag value will be 3, Reason code will be 98). On the second day, when the destination bank uploads the return file, then the response file generated and sent to the Sponsor Bank (on Day 2) will have file name similar to the normal response file, but, in addition, there will be a slight change in the sequence number. For example,

On Day 1, Response File received by the Sponsor Bank will be like APB-CR-HDFC-HDFC001-07062012-000001-RES.txt

On Day 2, Second response File received by the Sponsor Bank will be like APB-CR-HDFC-HDFC001-07062012-000001**-02-**RES.txt

The second response file will have all the transactions in the input file with their final status (including those of the destination banks which were not given extension. Transactions not returned by the destination bank will be shown as deemed accepted.

Mark Pending in ACH:

If a transaction is marked as pending, it means it is neither returned nor deemed accepted. The Destination Bank User wants to wait for some time to make a decision, so they mark the transactions in the return file as marked pending. They do this by giving the reason code 99. On giving a marked pending transaction the Destination bank User gets a time of one business day to make a decision regarding the transaction.

The number of times Mark Pending can be done is controlled through the Back End in a file called module.xml. So if max mark pending attempts is defined as 2, the destination bank user can mark his transactions as pending for a maximum of 2 business days. After which these transactions will get deemed accepted.

Currently, Mark Pending is not enabled in Production.

Validation of Files without Session

Files uploaded by banks and approved, will be validated and ACK will be sent immediately to the banks' mailbox. However, when the actual session is opened for the concerned product file, then the file is revalidated (like participant mapping on that day etc.) and DEL file will be generated for cancelled transactions.

For example, if Bank A uploads an ECS Credit Input File (with 10 transactions) for the value date as 19th September, is uploaded on 16th September. Bank B is the destination bank for 5 transactions and Bank C is the destination bank for the remaining 5 transactions. Now, the Input File will be validated and shown as Accepted. ACK will also be generated and sent.

On the value date, i.e. 19th September 2014, if, for some reason, Bank B is not participating in ECS Credit and is unmapped / blocked, when the ECS Credit session is opened for 19th, the Input File uploaded is revalidated and the transactions pertaining to Bank B will be cancelled. DEL File will be generated and sent to the Bank A, with details of the cancelled transactions.

Note:

- If however, multiple banks are unmapped/blocked, multiple DEL files will be generated (for each destination bank) per Input File uploaded.
- If, the entire file gets cancelled during revalidation, then no response file will be generated. Reconciliation will have to be done using the DEL file only.

2.4 APBS Process

There are two processes involved:

1. Aadhaar Seeding in the Mapper Database

2. Aadhaar Based Transaction Routing

Aadhaar Seeding in the Mapper Database

This process consists of mapping 12 digit Aadhaar numbers to Banks, by uploading Mapper File in NACH. The file flow of the same has been discussed in the earlier section. Mapper file format is detailed in a later section.

Aadhaar Based Transaction Routing

If only Aadhaar number is given in the file, then if that Aadhaar is available in the Mapper, the transaction will be routed to the respective bank.

If Aadhaar number and IIN are given in the file, then if that Aadhaar is available in the Mapper, and the IIN in the transaction file is the same as that available in the Mapper, then the transaction will be routed to the respective bank, else the transaction will be rejected.

The file naming details with example are provided below.

- Presentation Input File by Sponsor Bank

<Process Name>-<TransType>-<Bank Identifier>-<LoginId>-<Date>-<nnnnnn>-**INP**.txt

E.g. APB-CR-HDFC-HDFC001-07062012-000001-INP.txt

- Acknowledgement File to Sponsor Bank

<Process Name>-<TransType>-<Bank Identifier>-<LoginId>-<Date>-<nnnnnn>-INP-**ACK**.xml

E.g. APB-CR-HDFC-HDFC001-07062012-000001-INP-ACK.xml

- Inward File to Destination Bank

<Process Name>-<TransType>-<Bank Identifier>-<Date>-<nnnnnn>-**INW**.txt

E.g. APB-CR-ICIC- 07062012-000001-INW.txt

- Return File from Destination Bank

<Process Name>-<TransType>-<Bank Identifier>-<LoginId>-<Date>-<nnnnnn>-**RTN**.txt

E.g. APB-CR-ICIC-ICIC001-07062012-000002-RTN.txt

- Acknowledgement file to Destination Bank

<Process Name>-<TransType>-<Bank Identifier>-<LoginId>-<Date>-<nnnnnn>-**RTN-ACK**.xml

E.g. APB-CR-ICIC-ICIC001-07062012-000002-RTN-ACK.xml

- Output File to Sponsor Bank

<Process Name>-<TransType>-<Bank Identifier>-<LoginId>-<Date>-<nnnnnn>-**RES**.txt

E.g. APB-CR-HDFC-HDFC001-07062012-000001-RES.txt

File Format

The file formats are provided in Appendix 1 - NACH File Formats

File Sample

Sample Files are provided in Appendix 3 – Sample Files

NOTE: The files that are sent from upload/download screen to the application (ACH, MMS) have to be given a format of txt, xml or csv in the lower case. If .TXT, .XML or .CSV is given in upper case then SFG will throw an error and the file will not reach ACH.

3. Hardware and System Software

The ACH solution proposed has minimal requirement on banks side for setup. The solution is web based and can be accessed by the user through a secured channel of the bank with NPCI.

The key requirements for the bank user to login into the system and to upload the files are provided below.

3.1 Desktop

- PC with minimum one dual-core processor and 2 GB RAM
- Operating System – Windows XP or any other OS which supports the required browser and etoken drivers
- Network connectivity
- Browser – IE 8+, Firefox (latest)
- JRE – Java 6 runtime environment
- MIS reports are compatible in Internet Explorer (IE 32 bit) Browser, IE 8 and IE 9.

3.2 File Size and Record Size

File size – Input files

Assuming the size of each transaction for ACH of 306 characters in text file is 350 bytes, we have assumed three different file sizes for the calculation. The calculation is based on the number of records in the system.

The maximum size out of the file sizes mentioned below for ACH would be the limit set for each file uploaded onto the respective applications. Please note any file over the size will be rejected, so kindly ensure that the file is within the size limit provided below.

Assumptions taken

- ACH single record size is of 350 bytes in text file
- Maximum file size can be varied according to the file type. In NPCI_Custom.properties we defined the size for each type of file.

ACH Size of File

Input Txn size for one record =350 bytes

Txns Per File	File Size in KB	Signature Size	File Size in MB	File Size (Encoded XML file) in MB
10,000	3,418	6 K	3.3	Configurable from Back end
20,000	6,836	6 K	6.7	Configurable from Back end

3.3 Digital Certificates

- Class II Certificates for users of ACH & Class III Certificated for banks coming through Host-to-Host
- Procure certificates from IDRBT or any of the CAs approved by IDRBT
- Procure Standard Crypto tokens supporting PKCS#7

3.5 ACH File Signing using PKCS#7 Signature in Java

Steps Involved in Signing:

Creating Signature

Java Security packages can be used for the signature creation.

Following are the steps we need to follow for Signature creation.

1. Use a **PKCS** keystore (**pfx** file) (as specified by the certificate vendor)
2. Specify the Signature Algorithm (**SHA256WITHRSA**)
3. Read the file from system (original file)
4. Create an instance of **Bouncy Castle's CMSSignedDataGenerato**r call addSigner API by passing Private key, Certificate and Digest Algorithm(SHA256WITHRSA)
5. Create an instance of the java.security.Signature class with specified signature algorithm.
6. Use **initSign** method of java.security.Signature to initiate a signature with the private key of the user (private key extracted from the pfx file)
7. Use **update** method of java.security.Signature and pass the original file (without Base64 encoded)
8. Now use **sign** method of java.security.Signature which will return the signature in bytes

9. Now encode the signature with Base64 encoder
10. Extract the public key certificate from the keystore and encode it to Base64.
11. Encode the Original file also into Base64

3.6 Network Bandwidth

The bandwidth required for ACH application is 2 Mbps considering 2,00,000 ACH transaction per day.

3.7 Logic for Checksum

1. The main checksum validation method is using a string as its input. The detail of the string creation rules are provided below.
   - Fields considered for checksum at header level for the INW file are as follows - header control amount as an integer number (in paise), settlement date in dd/MM/yyyy format, header user number, receiver bank code (IFSC, MICR or IIN) and the item count as an integer.
   - Fields considered for checksum at record level for the INW file are as follows - record level amount as an integer number (in paise) , sponsor bank code (IFSC, MICR or IIN) , receiver bank code (IFSC, MICR or IIN), beneficiary account number or aadhaar number, user number, product type, UMRN (if no mandate, “NOTPROVIDED” to be considered as datavalue) and transaction reference number.
   - Fields considered for checksum at header level for the RES file are as follows header control amount as an integer number (in paise), settlement date in dd/MM/yyyy format, header user number, sponsor bank code (IFSC, MICR or IIN) and the item count as an integer.
   - Fields considered for checksum at record level for the RES file are as follows - record level amount as an integer number (in paise) , sponsor bank code (IFSC, MICR or IIN) , receiver bank code (IFSC, MICR or IIN), beneficiary account number or Aadhaar number, user number, product type, UMRN and transaction reference number.
2. The input string is transformed into an UTF-8 byte array.
3. For this byte array, hash digest is calculated, which is also a byte array.
4. Then, this byte array is translated into HEX characters
5. This is then converted into a base 16 number.
6. The number at 5 is then divided by 10000000000, and the remainder is used below.
7. This remainder can range from 0 to 9999999999. This number is right-padded with zeroes up to a length of 10 and returned as the checksum.

The Checksum validations are mentioned in the enclosed sheet

Checksum Validations.xlsx

3.8 Verhoeff Algorithm

The Mapper Files (ACH-AP) will use the Verhoeff Algorithm for calculating the checksum. All the other file formats will use the logic mentioned above in section 3.6.

4. Appendix

Appendix 1 – NACH File Formats

Following is the file format to be used for ACH, APBS, ECS and NECS files. These would be subsequently converted to ISO 20022 messaging standards.

The file format also includes ECS file formats including the revised return file format .The transaction codes to be used at header and record levels are specified in the file formats

Note: xsd, wherever attached herein, highlights the overall tag structure of the file. All the tags that are in xsd may not be used in NACH. The tags that are used in NACH, information on the same is available in the file formats document.

NACH file formats

ACH APBS ECS file formats.xls

XML ACH File Formats

ACH-APBS-XML FileFormat V1.2.xlsx

XML ACH XSDs

Debit xsd.zip Credit xsd.zip

Appendix 3 – Sample Files

ACH Files and Existing APBS Files

Samples-ACH-APBS-Files.zip

APBS Mapper File

Mapper Sample.zip

UID-Response File Foramt.xlsx

ACH Reject Reason Codes

ACH Reject Reason Codes.xlsx

Aadhaar Reject Reasons

AadhaarRejectReason2013-06-24 10-46-1

Appendix 7 – AV File Description, File formats and sample file

AV File Description

OMC will create account verification (AV) INP file and load in SFG with the destination bank as part of the file name. SFG will do technical validation and route the file to the destination bank. The destination bank will verify and upload the (AV) RES file which needs to be routed back to OMC. The vice-versa of bank originating and OMC confirming will also happen.

AV File format

AV File FormatsV1.1.xlsx

AV Sample File

AV Sample Files.zip

Appendix 8 – New Mapper formats and sample file

With the existing Mapper file format the following fields are added.

1. OD Flag
2. Mandate Flag
3. OD Date

OD Flag:

1. This flag will be used to indicate that a particular Aadhaar Number has availed an OD facility with any Bank, under PMJDY scheme.

2.The Bank enabling OD for an Aadhaar, will do so by uploading a mapper file with the OD flag as 'Y' for that Aadhaar.

3. Once an OD is enabled for an Aadhaar, any other bank updating the same Aadhaar will not be allowed.

4. OD Date should be mandatorily provided when OD flag is enabled / disabled.

5. Mandate Flag should be 'Y' when OD flag is updated.

Mandate Flag:

1. This flag will be used by the Bank to indicate that the customer has given the mandate for seeding to the corresponding Bank.

2. For any updating, Mandate Flag will have to be uploaded with value 'Y'.

3. Only for the first time Mandate Flag with value as 'N' will be allowed. Else, the same will be rejected.

New Mapper File Format

NACH Mapper file format V 2 1.xlsx

New Mapper Sample Files

ACH-CM MAP Files.zip