Data Exchange Module (DEM) for CTS – Technical Specifications Document

Version: 1.0

May 08, 2018

Table of Contents

1. OVERVIEW 3
- **a. Context** 3
- **b. Purpose of the Document** 3
- **c. Component Diagram** 4

2. Functional Requirements 5
- **a. Registration of DEM** 5
- **b. Submitting Outward Files** 8
- **c. Retrieving Inward Files** 11
- **d. Switchover of CH** 15
- **e. Resend of Files** 15
- **f. Data Reconciliation** 17

3. SECURITY 18
- **a. Secure Exchange** 22
- **b. PKI for Data in Transit** 22
  - **i. Outward Files** 22
  - **ii. Inward Files** 24
- **c. Dynamic Key Seeding and Revocation** 26

4. NON-FUNCTIONAL REQUIREMENTS 28
- **a. Performance** 28
- **b. Architecture** 28
- **c. High Availability** 28
- **d. Resilience** 29
- **e. Auditing and Logging** 29

5. Appendix-1 30

1. OVERVIEW

a. Context

Cheque Truncation Solution (CTS) hosted by NPCI is intended to provide cheque settlement and clearing services to banks in India. The solution is live in the country with existing model of Clear House (CH) and Clearing House Interface (CHI).

The CTS solution is planned for an upgrade in year 2018. With this upgrade, CH is made capable to provide business functionalities of CHI centrally. This provides option of replacing CHI with a low-cost Data Exchange Module (DEM) to the banks.

Below are the key functionalities expected from DEM:

- Upload outward files to CH after signing and encryption
- Download inward files and masters from CH and make them available to Capture System after signature verification and decryption
- Provide file reconciliation information to CH periodically
- Perform switchover to secondary CH as and when DR is invoked at CH
- Perform key and certificate exchange with CH to ensure usage of valid keys for file exchange

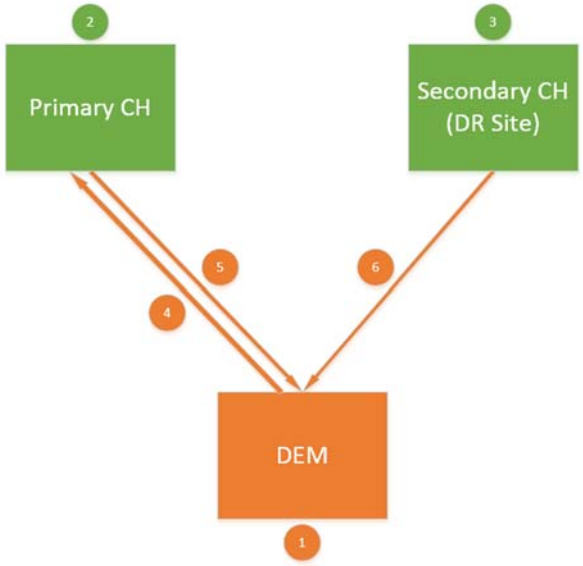
b. Purpose of the Document

The Data Exchange Module (DEM) is offered as an open specification option to the banks as opposed to existing single vendor CHI. This empowers banks to opt for vendor of their choice to provide DEM or develop and maintain in-house.

This document is intended to provide detailed specifications of DEM as a guideline to realize the same. The specifications in this document are categorized in two buckets:

1. Mandatory: These are required to be implemented for a smooth exchange of data with CH. Such specifications are given in **bold**.
2. Optional: These are guidelines for efficient and elegant functioning. Such specifications are given in normal text.

c. Component Diagram



Note: Banks can have multiple DEM installed and operational.

Legend	Description	Details
1	Data Exchange Module (DEM)	Software component owned and operated by Bank at their premises. Responsible for PKI security and data exchange with CH
2	Primary CH	GRID CH from where processing is live
3	Secondary CH	GRID CH as DR site to primary CH
4	Presenting outward files	DEM pushes outward files by sending a HTTPS message followed by SFTP of actual files
5	Receiving inward files	DEM monitors remote folders at Primary CH for available inward files and pulls the same to bank location over SFTP as and when available
6	Monitoring and processing DR	DEM monitors folder at Secondary CH for DR switchover file and swaps between primary and secondary sites as and when switchover is signaled

2. Functional Requirements

a. Registration of DEM

Being a financial system, it is mandatory to white list each individual installation of DEM at CH. CH will not exchange files with an un-registered DEM. This section details the registration process along with requirements to be implemented at DEM.

ID	Details	Owner

1.	It is mandatory for banks to submit a registration request for each DEM installation with mandatory fields filled in. Separate web-portal will be hosted by NPCI for this purpose.
	Following is the list of fields for registration of a DEM installation. Mandatory fields are denoted by *.
	• DEM Name
	• DEM ID
	• Bank Routing Number *
	• Access Identifier *
	• Access Type *
	• IP Address *
	• Primary & Secondary PKI certificates *
	• SFTP login credentials *
	• Contact details: *
	  o Name
	  o Email
	  o Phone Number
	• DEM Vendor *
		Bank

2.	**DEM Name:** Display Name for the DEM. This will be assigned by NPCI during approval of registration request and is non-editable field for banks.	
3.	**DEM ID:** Auto generated by CTS application.	
4.	**Bank Routing Number:** Routing number of the bank as per CTS masters for the GRID	
5.	**Access Identifier**: This can be one of the following: Bank Routing number: Routing number of the bank as per CTS masters for the GRID in case the DEM is expected to process outward and inward for the entire bank. Branch Routing Number: Nine-digit branch routing number as per CTS masters for the GRID in case the DEM is expected to process outward and inward for a specific branch of a bank. City Code: Valid city code from the GRID CH masters for which the DEM is expected to process outward and inward. In case the DEM is expected to process inward for multiple cities, please provide city code of primary city.	

	Transaction Code: Valid transaction code from the GRID CH masters for which the DEM is expected to process outward and inward. *Note: The access identifier will be used to provide access to the respective inward files. Hence, appropriate inward breakup option should be requested to CH to support this. E.g., in case the Access Identifier is a branch, the breakout option should be set to branch at CH. Similarly, if the Access Identifier is a City, the breakout option should be set to City at CH.* *In either scenario, bank is expected to provision DEM for each branch or City, as applicable.*	
6.	**Access Type**: Shall be one of the following: • Bank • Branch • City • Transaction Code	
7.	**IP Address:** The IP address which will be used for sending HTTPS messages and SFTP requests. *Note: This IP address will be whitelisted at CH. Hence, should be the same as which will be used in the requests. IP NAT, if any, should be considered while providing this value.*	
8.	**Primary & Secondary PKI certificates**: Certificates to be used for PKI security. Please refer Security requirements for details of the certificate format.	
9.	**SFTP login credentials**: user ID and password for SFTP login. The SFTP user ID shall be unique across all registered DEMs.	
10.	**Contact details**: Contact details of the responsible person – Name, email and phone number	
11.	**DEM Vendor**: Name of the vendor who is providing DEM. The list of known vendors will be readily available in drop down to choose from. In case the vendor is not available, please select "Other" and enter the name in text box provided.	
12.	After receiving the registration request at CH, NPCI shall verify and process the registration. A unique URL will be provided on the same UI as approval to the registration request.	CH
13.	**After the installation and configuration is completed at bank premises, bank must access the unique URL to activate the registration. DEM cannot exchange data with CH unless the installation is activated.** **It is mandatory to access the URL from the IP address provided during registration process.** ***The URL provided is unique per registration request and can be used only once.***	**Bank**
14.	Accessing the URL will provide following details to the bank: • IP address to send HTTPS message to Primary CH • IP address to send HTTPS message to Secondary CH • List of IP addresses to send SFTP requests to Primary CH • List of IP addresses to send SFTP requests to Secondary CH	CH

	• SFTP folder name at remote location to exchange inward and outward files • SFTP directory location to download Clearing House Masters (CHM) file • URL to access CH for HTTPS messages and key exchange in the format: "https:\\CH/token1/token2…. o Same URL needs to be used to communicate to CH by replacing "CH" with primary or secondary CH IP, as applicable	
15.	Above details needs to be configured in DEM for future usage.	Bank
16.	This completes the registration process for DEM.	

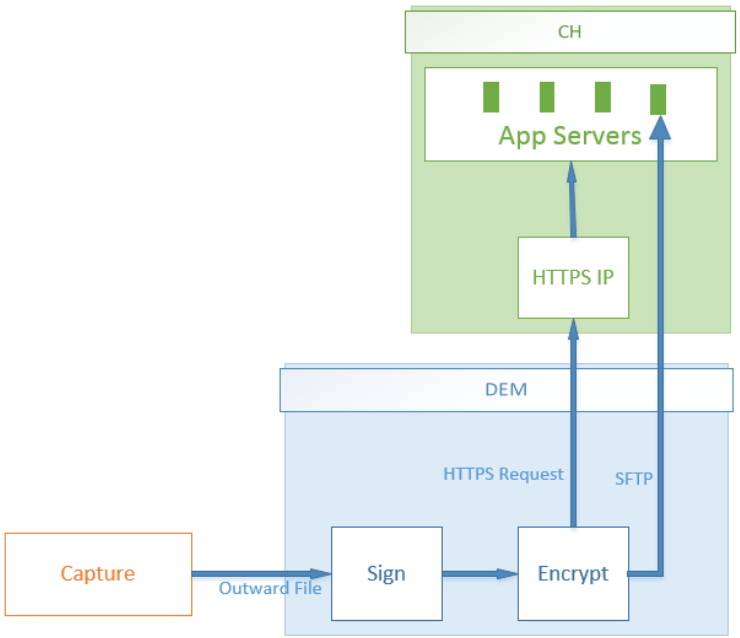
b. Submitting Outward Files

Outward files are the files coming from Capture System and to be submitted to CH for further processing. Below is the list of such files.

Important: The details of individual file naming and format requirements are available in CHI Specifications document. Please refer the same for further details.

File Type	Details
CXF	Outward presentment file containing details of items
CIBF	Outward presentment file containing images of the items in a CXF. Each CIBF is corresponding to a CXF and cannot exist on its own as independent file
RRF	Outward return file containing details of items to be returned
DONE	DONE files are used to indicate that transmission of a given file is completed. It is required that DEM shall create a DONE file for each file transmitted to CH. DONE file is a zero-kb file created by appending ".DONE" to the name of the file which is transmitted successfully by DEM

Below diagram provides the steps involved in uploading outward files to CH:



ID	Details	Owner
1	DEM will receive the outward files from Capture System.	Bank
2	DEM shall have no or minimum delay to pick up the files from Capture	Bank
3	DEM shall digitally sign the entire contents of individual file using bank's private key. Please refer Security requirements for details of digital signing. Sample content of a file after signature are as given below: Trans.Signature.Data Alias=X-167CHG_Syetmcert ThumbPrint= Routing_Number=070100 Sign-Algo=SHA256 Data=pw/OWTGGozX4tHwiBDFYNVGSECZLmzFuGWYgsD9Y2OgQYQ/gz7C/Yg3EP726Gf+2tCZLwKkRxF1TKgx5QyOLQiKrS94bxX/ruCx9qjOoI8TRp41lv1ZIhBs +dOHtoJ+MA6Ov7sqBn4QnxTWVmHruNgA1u5dh3qp3KPDLSMDLY5crKrLEzXW8z7AhgQo7lUV4jqdhIPL4/AOt/nzm4Fjwy84n9Ep7nYMAy8nfRdx7Nwhu7gg2rLa wkiEMcmCIJDqI7H5/6qxRrxYg== Trans.Signature.Data== ï»¿<?xml version="1.0" encoding="utf-8"?> <FileHeader xmlns="urn:schemas-ncr-com:ECPIX:CXF:FileStructure:040001" VersionNumber="040001" TestFileIndicator="P" Creation FileID="0023120"> <Item ItemSeqNo="00000001780826" PayorBankRoutNo="040100" Amount="1239703" AccountNo="9040002394787" SerialNo="461142" Tra PresentmentDate="02012018" CycleNo="01" NumOfImageViews="2" ClearingType="01" DocType="D" CurrencyInd="GHS" IQAIgnoreInd="0" TruncatingRTNo="000000" SpecialHandling="00" RepresentmentCnt="0" MICRRepairFlags="000000"> <AddendA BOFDRoutNo="070100" BOFDBusDate="17012018" DepositorAcct="999999" /> <ImageViewDetail ViewFormat="TIFF" CompressionType="JPEG" ViewSideIndicator="Front Gray" ViewDescriptor="Full" ImageAvai ReplacementDocIndicator="N" ImageCreatorRoutNo="901020" ImageCreationDate="17012018"> <ImageViewData ImageDataLength="0000109433" ImageDataOffset="0" FileName="CIBF_070100_17012018_192542_01_0023120_1.IMG ImageReferenceData="20180117090102011801171020001 9" ClippingOrigin="0" /> </ImageViewDetail> <ImageViewDetail ViewFormat="TIFF" CompressionType="JPEG" ViewSideIndicator="Back Gray" ViewDescriptor="Full" ImageAvail ReplacementDocIndicator="N" ImageCreationDate="17012018"> <ImageViewData ImageDataLength="0000054834" ImageDataOffset="109433" FileName="CIBF_070100_17012018_192542_01_0023120_ ImageReferenceData="20180117090102011801171020001 9" ClippingOrigin="0" /> </ImageViewDetail> </Item> Digital signing and encryption is not applicable for .DONE files as those are zero kb.	Bank
4	After successful signing, the entire contents including the digital sign shall be encrypted using public key of CH	Bank
5	After encryption, the file is ready to send. To initiate transmission, DEM must send a HTTPS message in following format: Request type: POST Request String: Reqtype=R&Filename=&Filetype=OUT&Filesize=&RouteId=&Timestamp=&HTTPSessionid=&FTPHostname= Where: Reqtype: Fixed value "R" Filename: name of the file to be sent in upper case. Comma separated list in case multiple files are to be sent. Max length: 256 char Filetype: fix value "OUT" Filesize: Size of the file in bytes. Comma separated list in case multiple files are to be sent. Max length: 256 char RouteId: DEM identifier Timestamp: Timestamp of the request, must not be a future time HTTPSessionid: For future use. To be kept blank. FTPHostname: For future use. To be kept blank.	Bank

6	This HTTPS request must be sent to the CH HTTPS URL received during registration process.	Bank
7	DEM shall wait for response of this message before initiating SFTP transmission.	Bank
8	As a response to the HTTPS request, CH shall send details in following XML format: <handshake> <errcode>0</errcode> <filetype>OUT</filetype> <reqtype>R</reqtype> <ftphostname>153.71.45.76</ftphostname> </handshake> Where: Errcode: Indicates processing result. Please refer appendix A for list of processing result codes and respective handling. Filetype: Fixed value OUT Reqtype: fixed value R Ftphostname: IP address of the FTP server to which SFTP connection shall be established.	CH
9	DEM shall not proceed with transmission if any of the following is true: 1. The HTTPS request timed out 2. Errcode has a non-zero value 3. Filetype and Reqtype values are not as expected 4. Ftphostname is not one of the SFTP server IP addresses provided by CH during registration process	Bank
10	After receiving valid response from CH, DEM shall establish the SFTP connection using login credentials set during registration process.	Bank
11	Upon successful connection, DEM shall send files listed in the initiation message to CH over SFTP with a temporary name. *Files received at CH are mapped against the names received in the corresponding message. Files not listed in the message will be ignored by CH*	Bank
12	After each file is transmitted successfully, DEM shall rename the file to its original name	Bank
13	It is advised to use temporary name by appending ".tmp" at the end of original file name. The ".tmp" string can be removed during the rename operation.	Bank
14	The file upload must be done to the folder location for file exchange received during registration process.	
15	After successful upload of files, the SFTP connection must be closed after logging out. Also, a timeout of 5min shall be set for idle/non-responding sessions. *Not closing the login session and SFTP connection can result in exhausting SFTP connections which will prohibit the DEM from sending files for duration set by NPCI.*	Bank

16	It is recommended that DEM shall implement timeout and retries for HTTPS messages and SFTP connection and transmission requests.	Bank
17	It is advised to send corresponding CXF, CIBF and .DONE files in a single HTTPS message to avoid delay in processing.	Bank
18	It is advised that DEM should keep a local backup of all uploaded files as CH may request them in future again.	Bank

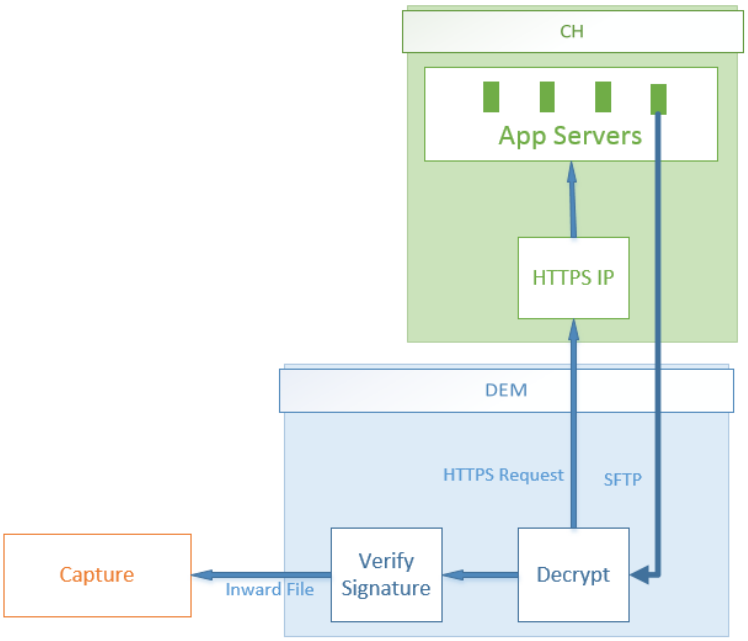
c. Retrieving Inward Files

Inward files are the files coming from CH and to be made available to Capture System for further processing. Below is the list of such files.

Important: The details about naming convention and file format requirements for Capture Interface files are available in CHI Specifications document. Please refer the same for further details.

File Type	Details
RES	Response file for already presented outward (CXF/RRF) file. There can be multiple response files for one presented file
PXF	Inward presentment file containing details of the items.
PIBF	Inward presentment file containing images of the items in a PXF. Each PIBF is corresponding to a PXF and cannot exist on its own as independent file
RF	Inward return file containing details of return items
EF	Inward Extension files containing details of extensions
OACK	Outward Acknowledgement file
EOS	End-Of-Session file
CHM	CH Masters file
CSV	CSV reports from CH
PDF	PDF reports

Below diagram provides the steps involved in retrieving inward files from CH:



ID	Details	Owner
1.	Periodically, DEM shall check for un-retrieved inward files to be present at primary and secondary CH and shall retrieve them, if present. To do so, DEM must follow following steps. *Note: In case of multiple DEMs at one bank, individual DEM is expected to scan respective sub-folders only. Please refer section "Multiple DEM for a Bank" for further details.*	Bank
2.	It is important that DEM should check and retrieve files from primary and secondary CH to support disaster or switchover scenario	Bank
3.	To initiate retrieval, DEM must send a HTTPS message in following format: Request type: POST Request String: Reqtype=R&Filename=&Filetype=IN&Filesize=&RouteId=&Timestamp=&HTTPSessionid=&FTPHostname= Where: Reqtype: Fixed value "R" Filename: blank Filetype: fix value "IN" Filesize: blank RouteId: DEM identifier Timestamp: Timestamp of the request, must not be a future time HTTPSessionid: For future use. To be kept blank. FTPHostname: For future use. To be kept blank.	Bank

4.	This HTTPS request must be sent to the CH HTTPS URL received during registration process.	Bank
5.	DEM shall wait for response of this message before initiating SFTP transmission.	Bank
6.	As a response to the HTTPS request, CH shall send details in following XML format: <handshake> <errcode>0</errcode> <filetype>IN</filetype> <reqtype>R</reqtype> <ftphostname>153.71.45.76</ftphostname> </handshake> Where: Errcode: Indicates processing result. Please refer appendix A for list of processing result codes and respective handling. Filetype: Fixed value IN Reqtype: fixed value R Ftphostname: IP address of the FTP server to which SFTP connection shall be established.	CH
7.	DEM shall not proceed with transmission if any of the following is true: 1. The HTTPS request timed out 2. Errcode has a non-zero value 3. Filetype and Reqtype values are not as expected 4. Ftphostname is not one of the SFTP server IP addresses provided by CH during registration process	Bank
8.	After receiving valid response from CH, DEM shall establish the SFTP connection using login credentials set during registration process.	Bank
9.	Upon successful connection, DEM shall check if there are any files present at the FTP folder locations received during registration process (for file exchange and for CHM) matching with file name pattern as given in the CHI specification document for inward files. *It is recommended to match maximum possible file name pattern to avoid overheads on DEM*	Bank
10.	It is mandatory to have the file types and paths configurable to ensure extensibility of the application. E.g., in future, DEM can be configured to transmit new file types as well or the folder structure can be changed.	Bank
11.	In case any such files are present, DEM shall download all files to local directory.	Bank
12.	DEM must download the files efficiently. Ideally, DEM shall retrieve one file in one FTP session. In case of multiple files per FTP session, the number of files to be retrieved per session must be configurable.	Bank
13.	Total count of FTP sessions a DEM can open with CH must be configurable and shall be set to the value advised by NPCI.	

14.	DEM must scan through all remote folders and subfolders to identify files to download *Note: for multiple DEM, the subfolder needs to be configurable per DEM installation. Please refer section "Multiple DEMs – Data Segregation" for further details.*	Bank
15.	DEM shall decrypt and verify signature of all files before making the files available to Capture System Decryption and Signature verification operations shall be configurable per file type. This is required to support zero KB files (e.g. EOS files) and other file types such as PDF and CSV. *Note: NPCI reserves the right to change the file types, naming convention and applicability of signing, encryption (one or both) for any inward or outward file type. Hence, this must be configurable.*	Bank
16.	After making each file available to Capture System, DEM must send HTTPS message in following format: Reqtype=A&Filename=&Filetype=IN&Filesize=&RouteId=&Timestamp=&HTTPSessionid=&FTPHostname= Where: Reqtype: Fixed value "A" Filename: name of the file which is downloaded in upper case including the relative subfolder path. Comma separated list in case multiple files are downloaded. Max length: 256 char Filetype: fix value "IN" Filesize: Size of the downloaded file in bytes. Comma separated list in case multiple files are downloaded. Max length: 256 char RouteId: DEM ID Timestamp: Timestamp of the acknowledge request, must not be a future time HTTPSessionid: For future use. To be kept blank. FTPHostname: For future use. To be kept blank.	Bank
17.	As a response to above HTTPS message, DEM must wait for following response before marking the retrieval as complete: <handshake> <errcode>0</errcode> <filetype>IN</filetype> <reqtype>A</reqtype> </handshake> For applicable error codes, please refer Appendix-1	Bank
18.	DEM must ensure that above HTTPS message is sent and response with errcode zero is received. This is required to ensure that same file(s) is/are not available for duplicate download. Any failure in this confirmation message exchange may keep	

	the file available for download and result in downloading same file(s) multiple times.	
19.	After successful download of files, the SFTP connection must be closed after logging out. Also, a timeout of 5min shall be set for idle/non-responding sessions. *Not closing the login session and SFTP connection can result in exhausting SFTP connections which will prohibit the DEM from sending files for duration set by NPCI.*	Bank
20.	DEM shall perform download activity sequentially in such a way that only one download is in progress for one file type at a given point in time. *Parallel download may result in corruption of files on disk*	Bank
21.	It is recommended that DEM shall implement timeout and retries for HTTPS messages and SFTP connection and transmission requests.	Bank
22.	It is recommended to have the time between two successive checks for inward files as configurable	Bank

d. Switchover of CH

ID	Details	Owner
1	During retrieval of inward files, DEM shall also check for switchover files at primary as well as secondary CH. A switchover file is a zero-kb file with naming convention DEMID_switchover.txt.	Bank
2	As and when the switchover file is received, DEM shall swap the IP addresses between primary and secondary CH. This shall result into DEM pointing to the secondary CH. *Note: Secondary CH is the CH to which DEM is not sending outward files. E.g., if a DEM in Western GRID is sending outward to Mumbai, the DR site i.e. Hyderabad becomes secondary. Similarly, when DEM is sending outward files to Hyderabad, Mumbai site becomes secondary.*	Bank
3	After swapping the IP addresses, DEM shall rename the remote file by appending ".processed" at the end of name of the file.	
4	The switch of IP addresses shall be applicable for HTTPS IP and SFTP server IP addresses.	Bank

e. Resend of Files

ID	Details	Owner
1	Depending on the processing at CH, occasionally CH can request DEM to resend certain files. This is required to handle scenarios of switch over and file getting corrupted during SFTP transmission.	CH
2	In such events, CH shall create a resend file and make it available in the SFTP folder location for DEM.	CH

3	Naming convention for resend file is DEMID_Resend.txt. This file contains list of files to be resend with one file name on each line. Below is a sample of contents: CXF_143123450_08052007_023102_00_0000866.XML CIBF_143123450_08052007_023102_00_0000866_01.IMG CXF_143123450_08052007_023102_00_0000867.XML CIBF_143123450_08052007_023102_00_0000867_01.IMG	CH
4	Optionally, the resend request file may contain time in minutes as first row in the file.	CH
5	DEM shall retrieve such files and as processing of this file, DEM shall first read list of files to resend and resend them to CH from local backup.	Bank
6	If the first two in the file is a time in minutes, DEM shall calculate the effective time by subtracting the minutes from current system time. e.g., if the resend file contents are as below: 90 CXF_143123450_08052007_023102_00_0000866.XML CIBF_143123450_08052007_023102_00_0000866_01.IMG CXF_143123450_08052007_023102_00_0000867.XML CIBF_143123450_08052007_023102_00_0000867_01.IMG DEM shall process as below: 1. Resend four listed files 2. Calculate effective time as: 18:00:00 – 90minuts = 16:30:00 Where 18:00:00 is current system time for DEM 3. Resend all files sent to CH after 16:29:59	Bank
7	As a final step of processing, DEM shall rename the remote file by appending ".processed" to the filename.	Bank

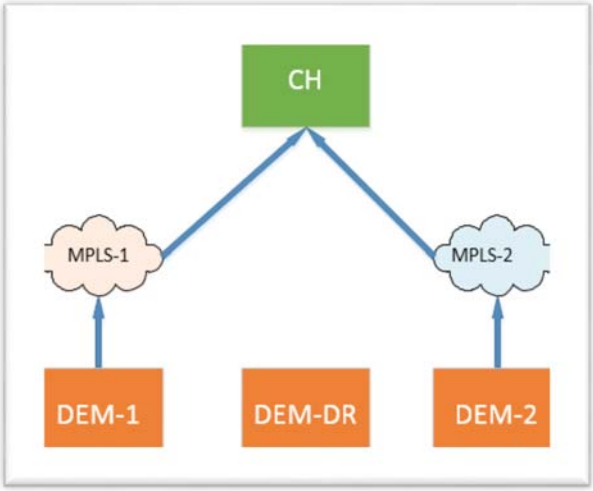
f. Data Reconciliation

<table>
<tr><th>ID</th><th>Details</th><th>Owner</th></tr>
<tr><td>1</td><td>For reconciliation, DEM must send count of presented and retrieved files to CH periodically.</td><td>Bank</td></tr>
<tr><td>2</td><td>It is required to send the reconciliation file at the end of each presentment or retrieval cycle.</td><td>Bank</td></tr>
<tr><td>3</td><td>Optionally, DEM can have an independent routine executed periodically to send the reconciliation file</td><td>Bank</td></tr>
<tr><td>4</td><td>Reconciliation file is a CSV file with naming convention as: DEMID_ddmmyyyy_HHmmss.dem.csv
Where, ddmmyyyy is date of creation of file and HHmmss is creation time.
HH indicates hour in 24 hr format
Single digit values should be left padded with zero (e.g. 1-Jan-2018 is written as 01012018)</td><td>Bank</td></tr>
<tr><td>5</td><td>The file shall contain a comma separated values which can be represented as below table:
<table>
<tr><th>FILE_TYPE</th><th>SESSION_NUMBER</th><th>FILE_COUNT</th></tr>
<tr><td>CXF</td><td>0</td><td>70</td></tr>
<tr><td>CIBF</td><td>0</td><td>70</td></tr>
<tr><td>PXF</td><td>1</td><td>12</td></tr>
<tr><td>PIBF</td><td>1</td><td>12</td></tr>
<tr><td>RRF</td><td>0</td><td>10</td></tr>
<tr><td>RF</td><td>2</td><td>5</td></tr>
<tr><td>RES</td><td>0</td><td>80</td></tr>
<tr><td>ERF</td><td>0</td><td>0</td></tr>
<tr><td>EF</td><td>0</td><td>0</td></tr>
<tr><td>EOS</td><td>1</td><td>1</td></tr>
</table>
File count for each file type is count of files sent or retrieved by DEM for the current System date.
Each file shall contain the header row as first row.
PXF indicates all types of PXF files.
For files which are not processed, entry with zero as file count is a must.</td><td>Bank</td></tr>
<tr><td>6</td><td>It is recommended to send reconciliation file every 30 seconds.</td><td>Bank</td></tr>
</table>

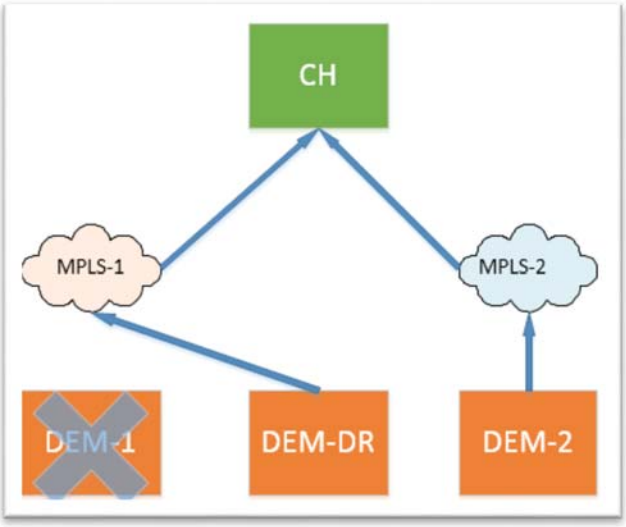
g. Multiple DEMs - Deployment models for a Bank

Banks are allowed to host multiple DEM in one GRID. In addition to serve with DR capabilities, this will also enable banks to utilize the redundant MLPS link efficiently. Below are the different models proposed in this regard:

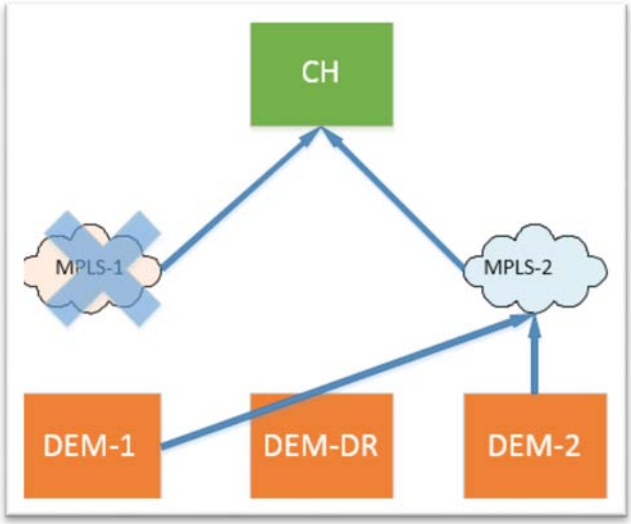
i. MPLS bandwidth optimization



DEM-1: DEM utilizing one MPLS link
DEM-2: DEM utilizing the other MPLS link
DEM-3: Common DR for DEM-1 & DEM-2



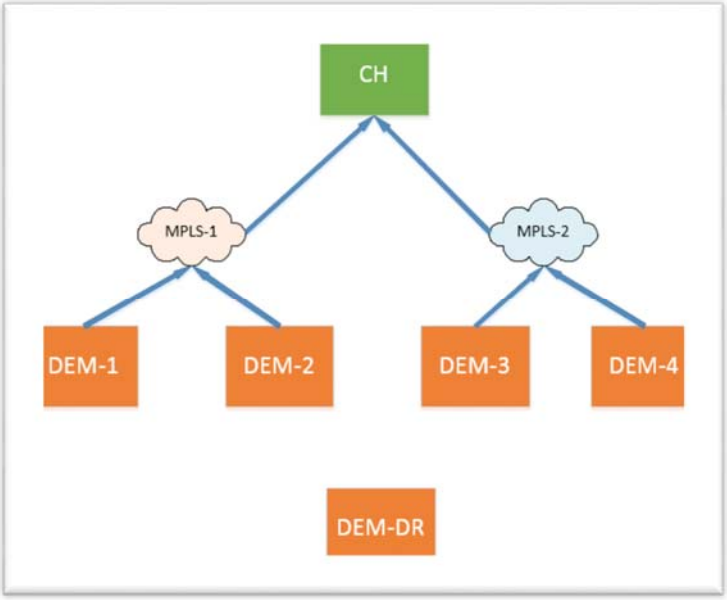
DEM DR



MPLS failover

ID	Details	Owner
1.	DEM-1 & 2 can process inward and outward in parallel by utilizing bandwidth from both MPLS providers	Bank
2.	In case of failure of any DEM, common DR setup can be made operational. Banks need to ensure data backup and replication across operational and standby DEM.	Bank
3.	In case of one MPLS link failure, both DEMs can be operated through another MPLS link	Bank

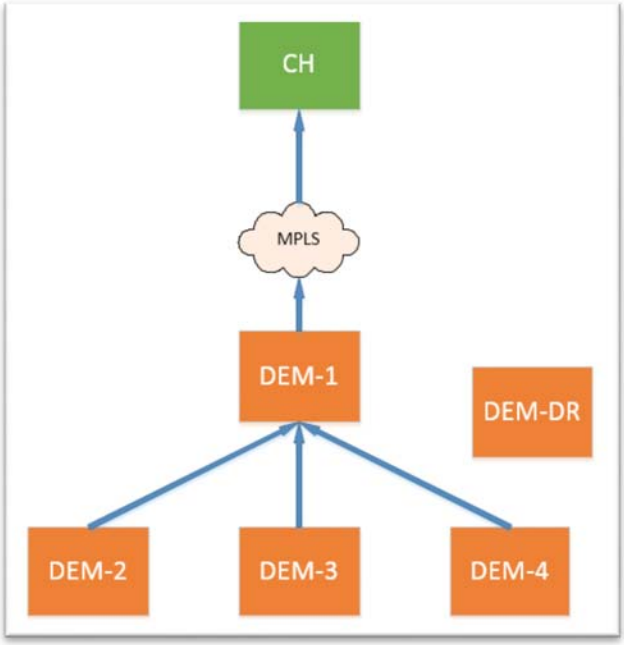
ii. Load Distribution



DEM 1 to 4: Active DEM responsible for respective inward and outward data exchange
DEM-DR: Common DR (Can be multiple)

ID	Details	Owner
1.	In this model, banks can opt to implement multiple DEM to exchange the data with CH	Bank
2.	The basis for segregation of data across DEM will be based on the operational model for the bank e.g., one DEM for each city, DEM for a group of cities, separate DEM for each transaction code etc.	Bank
3.	Bank can opt for single or multiple DR installations depending on total count of DEMs	Bank

iii. Spoke and hub



ID	Details	Owner
1.	In this model, internal DEM can connect with one (or two) DEM responsible for data exchange with CH	Bank
2.	In this model, the DEM installations internal to bank premises may not opt for PKI security.	Bank
3.	The DEM installations internal to bank will not be registered at CH	Bank
4.	This model can provide flexibility to banks to add DEM installations as and when required without any dependency on NPCI	Bank

h. Multiple DEMs – Data Segregation

ID	Details	Owner
1.	NPCI shall provide the bank folder access for all DEMs registered at CH for a given bank	CH
2.	For outward processing, each DEM must create a subfolder at CH for its outward submission. This is required to ensure that the same DEM should get the response files.	Bank
3.	For retrieval of inward files, each DEM shall be configured to access corresponding subfolders at CH. E.g., If the DEM is configured for given city or multiple cities, it must be configured to retrieve inward from folder for that city or cities only.	Bank

	Note: the folder structure for inward generation remains same as CHI i.e. bank/city/branch/date for city-wise inward generation, bank/branch/date for branch-wise generation and so on. *This configurability is currently available with captures as even today the inward is generated at central location and captures pick up relevant inward files for distributed processing model*	
4.	For DR DEM setup, adequate measures shall be provisioned to ensure back-up of local file system. This is to avoid the load on DR DEM as and when switchover is invoked.	Bank
5.	Each DEM exchanging data with CH must comply with the PKI requirements.	Bank
6.	Bank can opt for same or different PKI certificates for each DEM registered at CH	Bank

3. SECURITY

a. Secure Exchange

ID	Details	Owner
1	It is a must for DEM to use HTTPS protocol for message exchange. HTTP protocol will be blocked at CH.	Bank
2	It is must for DEM to use SFTP for file exchange. FTP and FTPS will be blocked at CH	Bank
3	It is must for DEM to use Hardware Security Module (HSM) for key storage, signing and encryption.	Bank
4	In memory encryption is not permitted for security reasons. The application is expected to send data to HSM card for signing and encryption on HSM card.	Bank
5	The port numbers for HTTPS and SFTP communication must be configurable at DEM.	Bank
6	DEM must support communication using TLS 1.1 and above.	Bank

b. PKI for Data in Transit

i. Outward Files

<table>
<tr><th>ID</th><th>Details</th><th>Owner</th></tr>
<tr><td>1</td><td>DEM shall use following security algorithms and topologies:
a. Hash algorithm RSA SHA-256
b. RSA Asymmetric encryption with 2048-bit key length
c. Triple DES (3DES, TDES) symmetric encryption with 168-bit key length
d. Certificates in X.509v3 format system certificate
e. Certificates must be stored in HSM card / network HSM
f. Bank public key certificate to be shared with CCH during registration for Digital Sign verification & Data Encryption
g. It is bank's responsibility to register the certificate from UI at CH as and when new certificate is intended to be used.
h. Class 3 system certificate is required for digital signing issued by IDRBT CA.</td><td>Bank</td></tr>
<tr><td>2</td><td>Digital Signature header information is as given below:
<table>
<tr><th>Line No</th><th>Content</th><th>Comments</th></tr>
<tr><td>1</td><td>Trans.Signature.Data</td><td>Start of signature header</td></tr>
<tr><td>2</td><td>Alias=X-167CHG_Syetmcert</td><td>It is Banks Private key label (Alias name) created in HSM card</td></tr>
</table></td><td>Bank</td></tr>
</table>

3	**ThumbPrint=**	**This is blank in case of HSM PKI operations.**
4	**Routing_Number=070100**	**Where 070100, is Banks DEM ID**
5	**Sign-Algo=SHA256**	**Digital signature algorithm name**
6	**Data= pw/OWTGGozX4tHwiBDFYNVGSECZLmzFuGW…**	**Digital Signature data**
7	**Trans.Signature.Data==**	**End of signature header**

Sample screenshot of Digital Signature header is given below:

```
Trans.Signature.Data
Alias=X-167CHG_Syetmcert
ThumbPrint=
Routing_Number=070100
Sign-Algo=SHA256
Data=pw/OWTGGozX4tHwiBDFYNVGSECZLmzFuGWYgsD9Y2OgQYQ/gz7C/Yg3EP726Gf+2tCZLwKkRxF1TKgx5QyOLQiKrS94bxX/ruCx9qjOoI8TRp41lv1ZIhBsciVhuO8MraQaTDSRqHdEVD+iDj6
Trans.Signature.Data==
```

3 Encryption header information is as given below: — Bank

Line No	Content	Comments
1	Trans.Encrypt.Data	Start of Encryption header
2	Alias=X-167CHG_Syetmcert	It is Banks Private key label (Alias name) created in HSM card
3	ThumbPrint=	This is blank in case of HSM PKI operations.
4	Routing_Number=070100	Where 070100, is Banks DEM ID
5	Algo=3DES	Encryption algorithm name. 3DES/TDES
6	Key=F0SFCV8Ziof+j3oSRgfVrVMiDDlUllYMq2I+yoZdlMLyA1D2b1b1N+GwaeU…	RSA Encrypted Symmetric Key which is wrapped in base 64 encoding. CH Public key is used for Encryption of symmetric key. Symmetric key is used for encrypting Digitally signed data.
7	Trans.Encrypt.Data==	End of Encryption header

Below is sample screenshot of encryption header:


```
Trans.Encrypt.Data
Alias=X-167CHG_Syetmcert
ThumbPrint=
Routing_Number=070100
Algo=3DES
Key=F0SFCV8Ziof+j3oSRgfVrVMiDD1U1lYMq2I+yoZdlMLyA1D2b1b1N+GwaeU5hdoDAxn0sQzyWOusqnnr1AR8ypQYCC6ZmpJo2oTb0fUJXHsveTbDQVvHpI+cYa2g0wffFcUDVZQWtnh1AFAlVek
Trans.Encrypt.Data==
```


ii. Inward Files

ID	Details	Owner
1	Encryption Header information is given below:	CH

Line No	Content	Comments
1	Trans.Encrypt.Data	Start of Encryption header
2	Alias=28CHG_System_PKIUtility	It is CH Private key label (Alias name) created in HSM card
3	ThumbPrint=4549E13331FFDCA6176262BC8B64EA0329873E39	This is CCH Public certificate thumbprint
4	Routing_Number=000100	Where 000100, is CCH Routing number
5	Algo=3DES	Encryption algorithm name. 3DES/TDES
6	Key=WuSsO1t0LdRvkJjr8Ztl0fz2VtcH+usbSN/0LR5I10wXViN.....	RSA Encrypted Symmetric Key which is wrapped in base 64 encoding. Banks Public key is used for Encryption of symmetric key. Symmetric key is used for decryption of downloaded file.
7	Trans.Encrypt.Data==	End of Encryption header

Below is a sample encryption header:


```
Trans.Encrypt.Data
Alias=28CHG_System_PKIUtility
ThumbPrint=4549E13331FFDCA6176262BC8B64EA0329873E39
Routing_Number=000100
Algo=3DES
Key=WuSs01t0LdRvkJjr8Zt10fz2VtcH+usbSN/0LR5I10wXViNcSNagjTdzR1B2qn3wtLV0HCJsd7xTqxW+gyhabNmaZiP+E7SoVfhpa80rd0XUqzI28lhs4eOzsAF2IqJir3X79/A29KZjMSj+kKq
Trans.Encrypt.Data==
```


2 Digital Signature header details are given below: CH

Line No	Content	Comments
1	Trans.Signature.Data	Start of signature header
2	Alias=X-167CHG_Syetmcert	It is CCH Private key label (Alias name) created in HSM card
3	ThumbPrint= 549E13331FFDCA6176262BC8B64EA 0329873E39	CCH public certificate thumbprint
4	Routing_Number=000100	Where 000100, is CCH Routing number
5	Sign-Algo=SHA256	Digital signature algorithm name
6	Data= MbzfPY8WVjXIOrsm/cmMJi9cm9DFkmlac7ZQxAykK0N89	Digital Signature data
7	Trans.Signature.Data==	End of signature header

Below is a sample digital signature:


```
Trans.Signature.Data
Alias=28CHG_System_PKIUtility
ThumbPrint=4549E13331FFDCA6176262BC8B64EA0329873E39
Routing_Number=000100
Sign-Algo=SHA256
Data=MbzfPY8WVjXIOrsm/cmMJi9cm9DFkmlac7ZQxAykK0N89jAmgC++ne7iUNjM4pmB+N+gV91QX51iRjj6tudwcD3GOga6s0m1gP2XMygEuoLpgMY22Hm0RA8cI+WaogQYYfKXZkAD4dKvwD4eIL
Trans.Signature.Data==
```

c. Dynamic Key Seeding and Revocation

ID	Details	Owner
1	DEM requires following keys for various PKI operations: a. Private key of DEM which is accessed by alias name created b. Public key of CH	Bank
2	At bank, the private keys for DEM are stored on HSM card / network HSM and the key alias name is stored at CH during certificate registration	Bank
3	At application startup, DEM shall make a HTTPS call to retrieve the CH public key and key alias name for bank key. The URL to send the HTTPS request will be provided by NPCI at later stage.	Bank
4	The request format is: Reqtype=W&DemId=DEMID&refreshInterval=4 Where, Reqtype: Constant value "W" DemId: DEM ID used during registration of DEM instance refreshInterval: Constant value "4"	Bank
5	The response format is: <handshake> <errcode>0</errcode> <reqtype>W</reqtype> <CCH_modulus>rFb+v7aHaZrnf6WvPJ2o5YZgPAkEBcPOPFuzIHA1/OIGsHMtt2y3tRrDS2s CW7eW2v6Qu+O4CGWER1zJ8fnkL8o2CvKI0/QhrrjAXD7B/nZ+qD7K1iq6yV9d9Nps4YgWB p8fMiwjO6cDcKhcVNI0mMSiCzpihnYoq0Bk1by+Xo0Dw7w+RnlyPfLulLHaPPXDh1R/nfIdypn olY8Po3LP8/EeCYeDEybRTMC4s21s/0WhS+KDF3lV73XKbyz3XYVkFH6SVMDEzIi3fN006z ZBZJPxXqyzEdhpIP8XlsOwQ9oDGHrAdqrRMMzj6Axzxd5tVC6iI4OD+ijTpl9iXEPT8Q== </CCH_modulus> <CCH_exponent>AQAB</CCH_exponent> <CCH_validfrom>2018-04-10 00:00:00.0</CCH_validfrom> <CCH_validtill>2020-01-01 00:00:00.0</CCH_validtill> <CCH_thumbprint>F1A73DD3F0781BAEF0CF6E8534056C189DA100C1</CCH_thumbprint> <DEM_validfrom>2018-03-15 00:00:00.0</DEM_validfrom> <DEM_validtill>2023-12-21 00:00:00.0</DEM_validtill> <DEM_thumbprint>A2B44B5258B5F88DD5B305C382EC93512727BD50</DEM_thumbprint> <DEM_keyaliasname>ecpix_77_19032018</DEM_keyaliasname> </handshake>	CH
6	The response fields are as detailed below: ID | Tag name | Description 1. | handshake | Start of response tag	CH

	2.	errcode	Errorcode=0 means Positive response Errorcode not 0 means negative response		
	3.	reqtype	For key exchange "W" request type is used.		
	4.	CCH_modulus & CCH_exponent	This both values are used to get CCH public key value from HSM card.		
	5.	CCH_validfrom & CCH_validtill	CCH Certificate validity period		
	6.	CCH_thumbprint	For future use.		
	7.	DEM_validfrom & DEM_validtill	DEM Certificate validity period		
	8.	DEM_thumbprint	For future use		
	9.	DEM_keyaliasname	It is use to identify private key details from HSM card.		
7	DEM shall stop processing of files in case the HTTPS call fails or error code is non-zero.				Bank
8	At CH, 1. Public key is refreshed at interval of 4hours 2. Certificate Revocation List (CRL) are updated at interval of 4hours Hence, it is mandatory for DEM to refresh the keys every 4hours minimum to ensure un-interrupted operation of DEM.				Bank
9	It is recommended to have key exchange automated at DEM.				Bank

4. NON-FUNCTIONAL REQUIREMENTS

a. Performance

ID	Details	Owner
1	DEM shall be designed to process required daily volumes for the bank	Bank
2	As a standard design basis for CTS, DEM shall be capable of processing 40% of daily volume of the bank in one hour. This shall include processing from sending the initiation HTTPS message till closure of SFTP session	Bank

b. Architecture

ID	Details	Owner
1	DEM shall support scalable architecture. This should include vertical as well as horizontal scaling	Bank
2	The file exchange with CH shall be unattended and shall not require any manual intervention after the files are available from capture	Bank

c. High Availability

ID	Details	Owner
1	DEM shall support multiple DEM in single GRID functioning as active-active setups as detailed in section "Multiple DEMs – Deployment options" *The criteria for separation of data across multiple DEM is detailed in section "Registration of DEM"*	Bank
2	In addition, DEM shall support DR setup which can be one-to-one or common DR for all DEM in a GRID, 1. DR DEM shall be registered at CH with distinct DEM ID 2. It is bank's responsibility to ensure current certificates for primary and DR installations of DEM are in sync and are registered at CH 3. DEM must be capable of replicating the retrieved files from one DEM to corresponding DR site. Files downloaded once will not be available for download again from CH. 4. Primary and DR DEM cannot process same file(s) in parallel as it will lead in corruption of files at CH. However, banks can have multiple DEM dedicated per branch or per city	Bank

d. Resilience

ID	Details	Owner
1	DEM shall be capable of processing the data 24 hours on a business day	Bank
2	DEM application shall sustain data processing for minimum of 24 hours without any restart or errors	Bank
3	The resource consumption of DEM shall be below 60% (or bank's corporate guideline, whichever is lower) of available resources.	Bank
4	DEM shall facilitate automated data and log clean-up	Bank

e. Auditing and Logging

ID	Details	Owner
1	DEM shall create an audit log for following: 1. All HTTPS communication with CH including the request and response contents 2. Various file operations such as: For outward: a. Receiving file from Capture b. Signing and encryption of file c. Start and end of SFTP transmission of individual file to CH d. Backup of a processed file For inward e. Start and end of retrieval for individual file from CH f. Decryption and signature verification g. Making the file available to Capture h. Renaming of the file at remote location 3. All configuration changes 4. Startup and shutdown of application 5. Any other tasks which DEM does	Bank
2	All audit logs must have details of DEMID, IP address, User ID, timestamp (up to seconds) as applicable.	Bank
3	DEM application shall log all errors occurred along with details of the operation and/or file being processed.	Bank

5. Appendix-1

List of Error Codes expected from CH

Error Code	Significance
0	Request processed successfully i.e. no error in processing
1	REQUEST_TYPE_NOT_FOUND i.e. invalid request type mentioned in the request (other than "R" or "W")
2	CCH_CERTIFICATE_INVALID i.e. valid certificate for CH is not found.
3	BANK_CERTIFICATE_INVALID i.e. valid certificate for Bank is not found.
4	CCH_BANK_CERTIFICATE_INVALID i.e. valid certificate is not found for CH as well as Bank. Please note that this error code is used for any error which is not covered by existing list of error codes.