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

Version: 14

May 26, 2023

Table of Contents

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 from CH and make them available to Capture System after signature verification and decryption
- Download master files (CHM) from CH and make them available to Capture System.
- 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

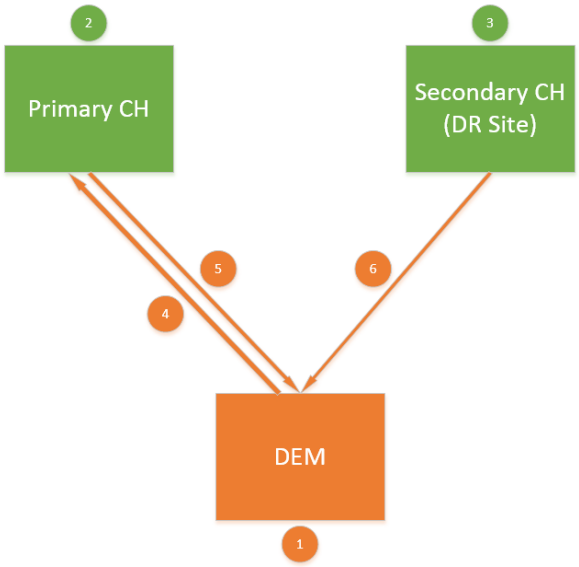
b. Purpose of the Document

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: *
	  ○ Name
	  ○ Email
	  ○ 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. It can be alphanumeric up to length 10 (VARCHAR 10)	
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. *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	
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 locations to exchange inward and outward files. Two separate FTP locations:
	  o Upload FTP location for Outward files
	  o Download FTP location for Inward 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

i. Outward Files from Capture system

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.

Bank DEM should not allow to present outward files for banks other than Self or Sub members under it (based on latest CHM). DEM should restrict the files at DEM itself and should not transmit to CCH.

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 to DEM from capture.

ii. Outward Files from CPPS Bank

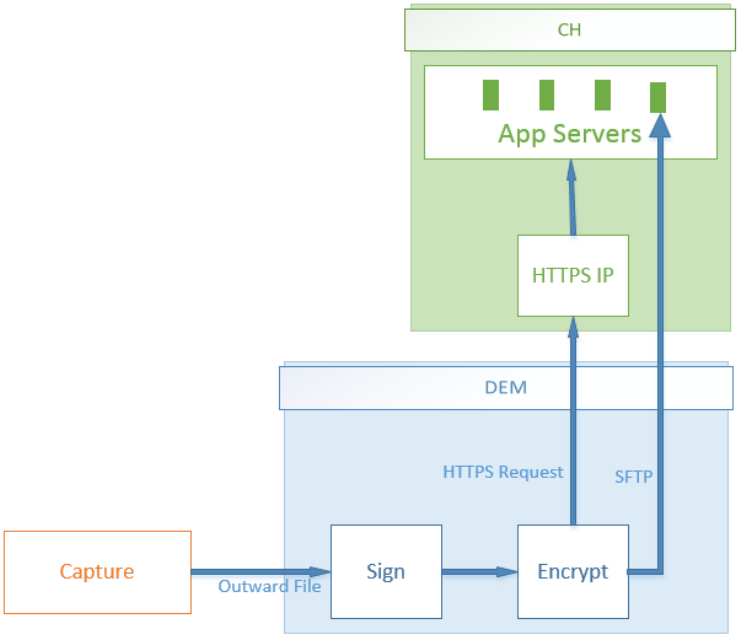
Outward files are the files coming from CPPS enabled Bank and to be submitted to CH for further processing. Below is the list of such files.

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

Bank DEM should not allow to present outward files for banks other than Self or Sub members under it (based on latest CHM). DEM should restrict the files at DEM itself and should not transmit to CCH.

File Type	Details
CIIF	Outward CPPS presentment file containing details of items.

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 and encryption 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="20180117090102011801171020019" 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="20180117090102011801171020019" ClippingOrigin="0" /> </ImageViewDetail> </Item>	Bank

<table>
<tr>
<td></td>
<td>Sample of CIBF file after signature and encryption:
Routing_Number=110300300
Algo=TDES
Key=OVkxJQdSV8Ek8r9FhAzow5zsmMmEgMbBxoJq/w9c4WJHGGj3VQlGK+f2+YAZl8wZ2tSMzbaGF/rQdenC9fVI/gN4aUG2Yenm1j3S
L5v40fLuaJBSQF/JI48MvMIYMU7/coHAx7N8eCnc7ZueW/rY0TxBp25+bWpVbmgOO0L9waejO/xHzWsjy4/j3etAdbowpbYYSvtwAA6p
WJVYLZXyGfHE691zqaT3tGGsenO7teyvnYKFbGKOAWEk2G3k/8zapGhaNzvBafBItXOAyARFrfq/b3OE9TvWIraBfEwr1Am4pTp1D/Wx
W5JpXTvy1jck3p5md+gQDAuPRUBBAZRGxQ==
Trans.Encrypt.Data==
Æþó7¡ƒÍÝ┘à ´Þ3L"²[T6Ù,,sÝr§÷Eœ`l¹=W°¯xî—tµ‼|.õ£åD5èÛŒs¸da©¶1—ç‼~á„wq›Ûp{JûÎ¶'I#Ììas_mTÍèhS™èÝÎN‹eùü
(Ïâµ¥b←Z◄|ëSŸ5h/Q¼¬6ûê¢:63:Í‰äöÐ®½|÷@ªÿ:gÔéÔ:äÇ–„ÂfÌOý¡¥¸Ï÷½¹,
¾»‡¼±ÛE¾T¼Ö³ØÅÇ‹ï³}-mž~¶Ý‼½°¯fØ'Ë×2Æ¿®┤|‰|dàŠ=ÎLÆç€¥ÆùÄ↑hWÖ×└€™¨Ê┬j ªª
┬êiÈÆ‼=nÛ´á±'Ó×↕0¶à?z£↑ý,¼Vÿ┐==zÓË¶\$a'├¢À┐L¼ÓpvÐöÏ,▮ª¤È^ENÃk¦9êœÐA‰ßbvóîy×1°)ßS,'¸\®D/ dÖÉÆŒ↑
Òqñ]°†ÐÌ»o2""æs÷zÙðÖSÎ‼┼Ûá¡kú—¾w°í2ò←|õPfçf¨D Û6Œ>d¹i◄>ÒlËßá┤Ür¡¡
ÓÁpÈÆx¤↑,¼<Ïk‰Î<Ð¿æ& ▯ï←Ý¶-•l° °kcç┴oÅ;ÓTXmçl┤XöÎ>ŠÙ‰½CP 3c+ →µŽ<"UÉÔ„Ÿ¯ì "E[¯ „Ê£‼┐é»ÊJ
/.+Œ→?@4ôáî$Tf" ªP&óÜfÚ
vµ4ß„\ü+›>þ }Ï&ü©Gðó,ÂA¸-"øÅ▯Årå→zÙ‹m-SÕÏõê‰WN¿-^‰1òd↑JÚq┐-…Éý|"´BóÔr┬k ë›®i)†Z—˜¿Ac•ÅO q
4
_Mßõ] ÏòÎ Ü›à,®ïcEØ·ÉZÖ
Q·e–▮ÔO LÊ¾{x}G5f→SöÏOÒ1…±@Ø├æ·9üußÎ‼ôûM;ßN-$>◄~#‹[© v^„›-Eà~$┴ý'$®!HBŽlúý2¬©¬]&ÄT['
"ž┼|▯ÔÔ–…uÔiÈ↑.7Å@hjÈ)ŠÍÂöf‰è¦Ý|þ‰WkŽ‡·
ú:‰xI ŒdÕ³æm"¨¤JeŒ ®é&è~·→"f–◄Lê^âLö^‰«"3©Z
Ð3ŽŸÑ–┐

Digital signing and encryption is not applicable for .DONE files as those are zero kb. DEM shall ignore .Done file.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>After successful signing, the entire contents including the digital sign shall be encrypted using public key of CH</td>
<td>Bank</td>
</tr>
<tr>
<td>5</td>
<td>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.</td>
<td>Bank</td>
</tr>
<tr>
<td>6</td>
<td>This HTTPS request must be sent to the CH HTTPS URL received during registration process.</td>
<td>Bank</td>
</tr>
<tr>
<td>7</td>
<td>DEM shall wait for response of this message before initiating SFTP transmission.</td>
<td>Bank</td>
</tr>
<tr>
<td>8</td>
<td>As a response to the HTTPS request, CH shall send details in following XML format:
<handshake>
<errcode>0</errcode>
<filetype>OUT</filetype></td>
<td>CH</td>
</tr>
</table>

	<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.	
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	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 upload FTP 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 and CIBF files in a single HTTPS message to avoid delay in processing. DEM should not upload .Done file to CH.	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

i. Inward Files for Capture System

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 from CH
XLS	XLS reports from CH
RPT	RPT reports from CH

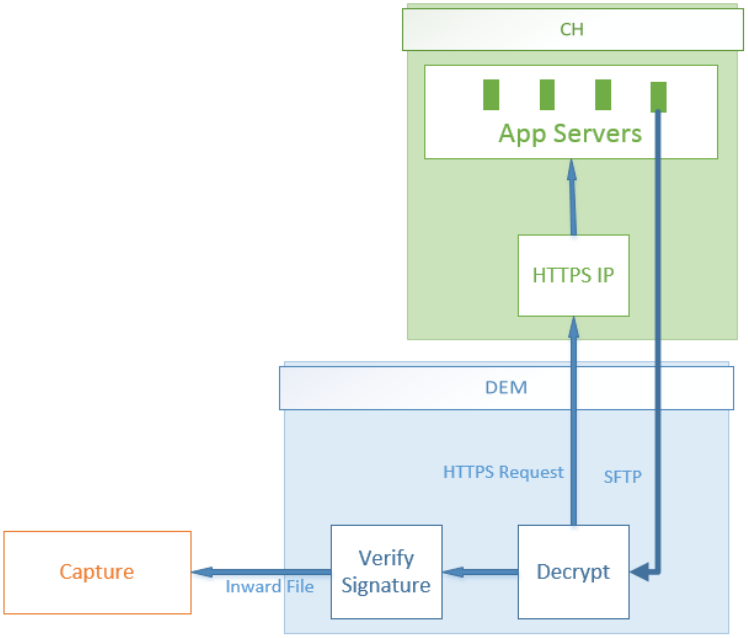
ii. Inward Files for CPPS Bank

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

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

File Type	Details
CPPS_RES	Response file for already presented outward (CIIF) file.

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	Bank

	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.	
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	Bank
8.	After receiving valid response from CH, DEM shall download files using following options, 1. Get download file list from remote directory scan using SFTP connection. 2. Get download file list using HTTPS message. *NOTE: 1) In case of single Bank DEM, they can use any one option at a time.* 2). In case of multiple DEMs where subfolders have been configured at CCH to segregate inwards file. They must use Option -2.	Bank
9.	1. Get File list from remote directory scan using SFTP connection: 1.1. DEM shall establish the SFTP connection using login credentials set during registration process. Upon successful connection, DEM shall	Bank

	check if there are any files present at the download 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*	
	1.2. 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
	1.3. 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
	1.4. In case any such files are present, DEM shall download all files to local directory.	Bank
	1.5. 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
	1.6. 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.	
	1.7. Total count of FTP sessions a DEM can open with CH must be configurable and shall be set to the value advised by NPCI.	Bank
	2. Get File list using HTTPS message: 2.1. Bank DEM should send intermittent HTTPS message to get list of available files for download. Request type: POST Request String : Reqtype=FL&Filename=&Filetype=IN&Filesize=&RouteId= Where: Reqtype: Fixed value "FL" Filename: blank Filetype: fix value "IN"	Bank

	Filesize: blank RouteId: DEM identifier HTTPS message Response: As a response to the HTTPS request, CCH send details in following XML format: If file is available for download, below will the response <handshake> <errcode>0</errcode> <filetype>IN</filetype> <reqtype>FL</reqtype> <File_List> 1123\CXF_070200200_20022018_164332_01_0001326.XML.RES;070200200\BPXF_070200200_20022018_164332_01_0001327.XML </File_List> </handshake> *NOTE: File_List will contain file name with relative path. In case of multiple files, it will be semi-colon separated.* If no file is available for download, below will the response <handshake> <reqtype>FL</reqtype> <errcode>0</errcode> <filetype>IN</filetype> <File_List>NO_FILES_FOUND</File_List> </handshake>	
	2.2. Using DEM identifier (ID), CCH DEM retrieve available valid files for download from DB. Number of available files that will be send for each HTTPS request will be configured by CCH. Default value is 100. *Note: In case of multiple DEM, Bank needs provide list of subfolders to CCH operator for configuration of subfolder as per DEM at time of installation.* *In future any changes in subfolders, CCH operator needs to be informed.* *Please refer section "Multiple DEMs – Data Segregation" for further details. As per subfolder configuration CCH DEM retrieve list of files for download.*	CCH

	2.3. Based on file list, Bank DEM shall prepare a Download batch of 5 files. Each download batch connect SFTP session & download the files. DEM download the file with temporary file name and after successful download, it renamed it back to original name.	Bank
	2.4. 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
10.	After downloading files per session, DEM must send HTTPS message in following format: Reqtype=A&Filename=&Filetype=IN&Filesize=&RouteId=&Timestamp=&HTTP Sessionid=&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. *Note: Bank DEM must send acknowledgement via http message to CCH for inward file as well as report files.*	Bank
11.	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-A	Bank
12.	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.	
13.	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). *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
14.	DEM shall perform download activity sequentially in such a way that only one download is in progress for one file at a given point in time. *Parallel download may result in corruption of files on disk*	Bank
15.	It is recommended that DEM shall implement timeout and retries for HTTPS messages and SFTP connection and transmission requests.	Bank
16.	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 where * can be alphanumeric string up to 35 characters. 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

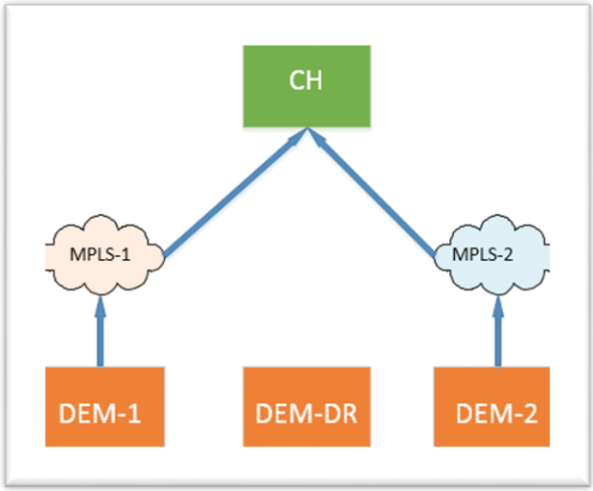
f. Data Reconciliation

<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>
<tr><td>CIIF</td><td>0</td><td>5</td></tr>
<tr><td>CIIF_RES</td><td>0</td><td>3</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.
CIIF and CIIF_RES file type applicable only for CPPS enabled Banks.</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>

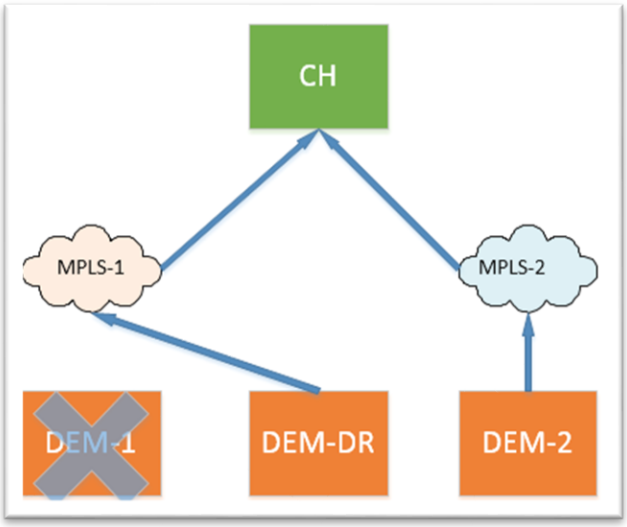
g. Multiple DEMs - Deployment models for a Bank

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:

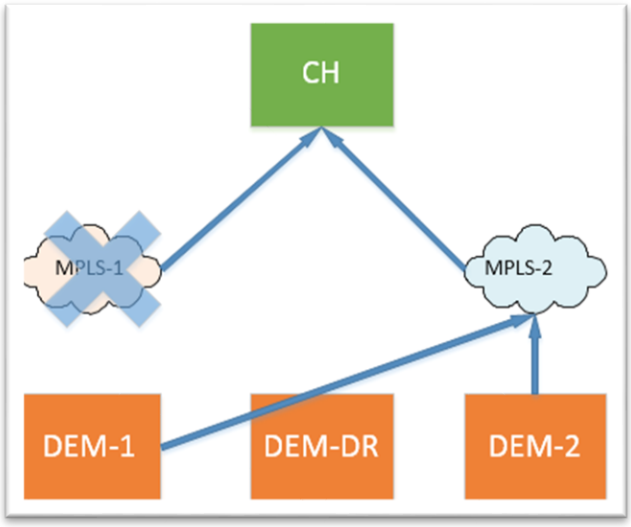
i. MPLS bandwidth optimization



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



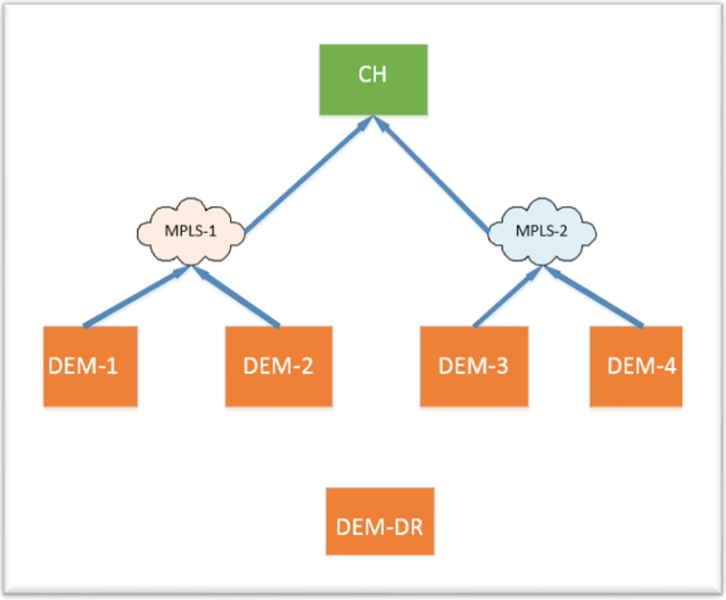
DEM DR



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

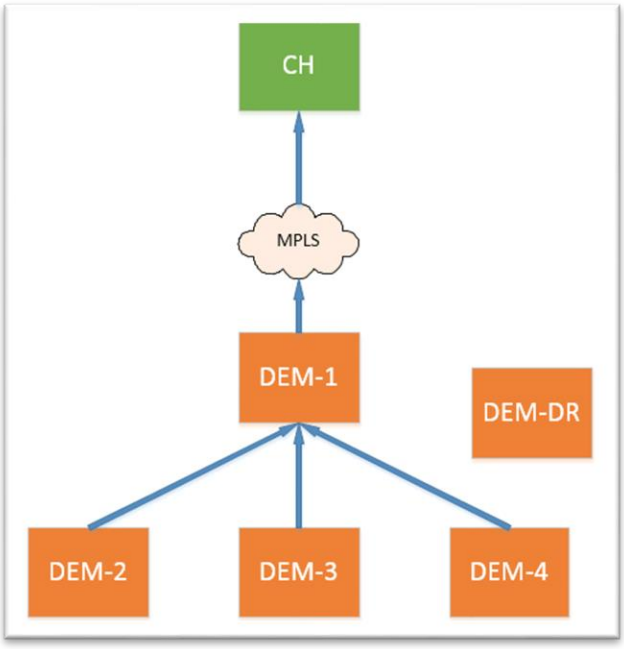
ii. Load Distribution



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>Supported Security algorithm:

3DES -Triple Data Encryption Algorithm is a way to reuse 3DES implementations, by chaining three instances of DES with different keys. 3DES is believed to still be secure because it requires 2^{112} operations which is not achievable with foreseeable technology. 3DES is very slow especially in software implementations because 3DES was designed for performance in hardware.

AES -Advanced Encryption Standard is the successor of DES as standard symmetric encryption algorithm. AES uses keys of 128, 192 or 256 bits, although, 128-bit keys provide sufficient strength today. It uses 128-bit blocks and is efficient in both software and hardware implementations.

Comparison:
<table>
<tr><th></th><th>3DES</th><th>AES</th></tr>
<tr><td>Key Length</td><td>56 bits</td><td>128, 192, or 256 bits</td></tr>
<tr><td>Cipher Type</td><td>Symmetric block cipher</td><td>Symmetric block cipher</td></tr>
<tr><td>Block Size</td><td>64 bits</td><td>128 bits</td></tr>
</table>
</td><td>Bank</td></tr>
</table>

Security	Proven inadequate	Considered secure
	Has shorter and weaker encryption keys compared to AES. Believed to still be secure because it requires 2^{112} operations which is not achievable with foreseeable technology.	More secure than the 3DES cipher and is the de facto world standard.

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. The Initialization vector must be a byte array initialized with value 0 to 7.
d. Advanced Encryption Standard (AES) with 256-bit key length. The Initialization vector must be a byte array value 0 to 16 for AES padding.
e. Certificates in X.509v3 format system certificate
f. Certificates must be stored in HSM card / network HSM
g. Bank public key certificate to be shared with CCH during registration for Digital Sign verification & Data Encryption
h. It is bank's responsibility to register the certificate from UI at CH as and when new certificate is intended to be used.
i. Class 3 system certificate is required for digital signing issued by IDRBT CA.
j. All conversion between Byte to string and vice versa shall be done using ASCII Encoding
k. Line separator character must be '\n' at following places,
    - Between encryption header and encrypted content
    - Between Signature header and File content

2 — Digital Signature header information is as given below: — Bank

Line No	Content	Comments
1	**Trans.Signature.Data**	**Start of signature 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=110001000**	**Where 110001000, is DEM Bank Routing_Number**
5	**Sign-Algo=SHA256**	**Digital signature algorithm name**
6	**Data= pw/OWTGGozX4tHwiBDFYNVGSECZLmzFuGW…**	**Digital Signature data. which is wrapped in base 64 encoding.**

	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/ruCx9qjOoI8TRp4l1v1ZIhBsciVhu08MraQaTDSRqHdEVD+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=**110001000**	Where **110001000**, is DEM Bank Routing Number
5	Algo=3DES	Where 3DES, is encryption algorithm name. For 3DES must be: 3DES / TDES For AES must be: AES
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+j3oSRgfVrVMiDDlUllYMq2I+yoZdlMLyAlD2b1b1N+GwaeU5hdoDAxn0sQzyWOusqnnrlAR8ypQYCC6ZmpJo2oTb0fUJXHsveTbDQVvHpI+cYa2g0wffFcUDVZQWtnhlAFAlVek`
	`Trans.Encrypt.Data==`	

4	Following outward file types are required to have signing and encryption: 1. CXF 2. CIBF 3. RRF 4. CIIF (Only for CPPS enabled Bank)	Bank
5	Following outward file types does not require signing and encryption: 1. Reconciliation file	Bank

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=110001000	Where 110001000, is CCH Routing number
5	Algo=3DES	Where 3DES, is encryption algorithm. For 3DES must be: 3DES / TDES For AES must be: AES
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:

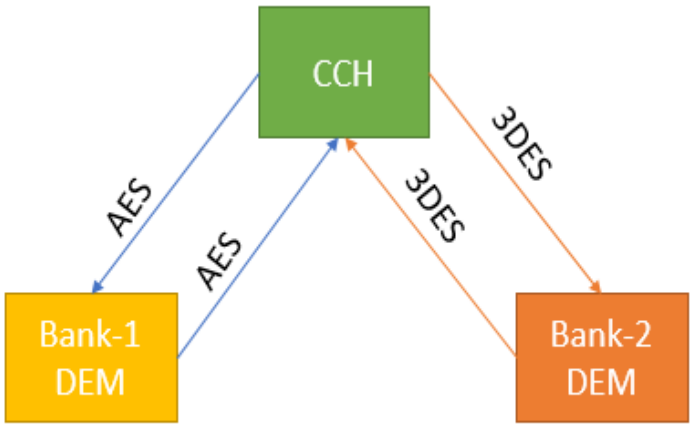
```
Trans.Encrypt.Data
Alias=28CHG_System_PKIUtility
ThumbPrint=4549E13331FFDCA6176262BC8B64EA0329873E39
Routing_Number=000100
Algo=3DES
Key=WuSs01t0LdRvkJjr8Zt10fz2VtcH+usbSN/0LR5I10wXViNcSNagjTdzR1B2qn3wtLV0HCJsd7xTqxW+gyhabNmaZiP+E7SoVfhpa80rd0XUqzI28lhs4eOzsAF2IqJir3X79/A29KZjMSj+kKq
Trans.Encrypt.Data==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

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=110001000	Where 110001000, is CCH Routing number
	5	Sign-Algo=SHA256	Digital signature algorithm name
	6	Data= MbzfPY8WVjXIOrsm/cmMJi9cm9DFkmlac7ZQxAykK0N89	Digital Signature data. which is wrapped in base 64 encoding.
	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+gV9lQX5liRjj6tudwcD3GOga6s0m1gP2XMygEuoLpgMY22Hm0RA8cI+WaogQYYfKXZkAD4dKvwD4eIL Trans.Signature.Data==	
3	Following inward file types are required to have signature verification and decryption: 1. RES 2. OACK 3. PXF 4. PIBF 5. RF 6. EF 7. CPPS_RES (Only for CPPS enabled Bank) 8. PDF (Report from CH) 9. RPT (Report from CH) 10. XLS (Report from CH) 11. CSV (Report from CH)	Bank
4	Following inward file types does not require signature verification and decryption: 1. EOS 2. RESEND 3. SWITCHOVER 4. CHM	Bank

iii. File encryption Interfaces:

The diagrammatic representation for file exchange interfaces with required encryption algorithms is given below:



Sr. No	Originator	Receiver	Encryption Algorithm
1	Bank-1 DEM	CCH	AES 256
2	CCH	Bank-1 DEM	AES 256
3	Bank-2 DEM	CCH	3DES
4	CCH	Bank-2 DEM	3DES

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,	Bank

<table>
<tr><td></td><td>Reqtype: Constant value “W”
DemId: DEM ID used during registration of DEM instance
refreshInterval: Constant value “4”</td><td></td></tr>
<tr><td>5</td><td>The response format is:
<handshake>
<errcode>0</errcode>
<reqtype>W</reqtype>
<CCH_modulus>rFb+v7aHaZrnf6WvPJ2o5YZgPAkEBcPOPFuzIHA1/OIGsHMtt2y3tRrDS2s
CW7eW2v6Qu+O4CGWER1zJ8fnkL8o2CvKI0/QhrrjAXD7B/nZ+qD7K1iq6yV9d9Nps4YgWB
p8fMiwjO6cDcKhcVNl0mMSiCzpihnYoq0Bk1by+Xo0Dw7w+RnlyPfLulLHaPPXDh1R/nfldypn
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></td><td>CH</td></tr>
<tr><td>6</td><td>The response fields are as detailed below:
<table>
<tr><th>ID</th><th>Tag name</th><th>Description</th></tr>
<tr><td>1.</td><td>handshake</td><td>Start of response tag</td></tr>
<tr><td>2.</td><td>errcode</td><td>Errorcode=0 means Positive response
Errorcode not 0 means negative response</td></tr>
<tr><td>3.</td><td>reqtype</td><td>For key exchange “W” request type is used.</td></tr>
<tr><td>4.</td><td>CCH_modulus & CCH_exponent</td><td>This both values are used to get CCH public key value from HSM card.</td></tr>
<tr><td>5.</td><td>CCH_validfrom & CCH_validtill</td><td>CCH Certificate validity period</td></tr>
</table></td><td>CH</td></tr>
</table>

	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-A

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.
9	DB_INSERT_ERROR i.e. Any DB operation failed at CH

6. ADFS Configuration and Work group configuration

a. Introduction:

NPCI has hosted a centralized UI for banks migrating from Clearing House Interface (CHI) to Data Exchange Module (DEM). The banks can access this UI to monitor processing at CH and to retrieve reports.

To access the centralized UI, banks need to carry user management locally. The user management can be done with either of the options:

1. In bank's corporate Active Directory (AD) with Active Directory Federation Services (ADFS)
2. By creating work group for DEM. This option can be used if bank does not have corporate AD or does not have access to corporate AD from DEM network or cannot provide ADFS due to any other reason.

Note: The ADFS can be configured on the AD server as additional role or can be installed as a service on a server which can access corporate AD.
For configuration details of ADFS with Active Directory, please refer b. Configuring CCH UI access using active directory.
For configuration details of work group, please refer c. Work Group user and Roles Creation

b. Configuring CCH UI access using active directory:

Banks need to execute following steps to configure user authentication and management using active directory and ADFS

Step-1: Configuration changes at active directory:

Banks are required to configure following user attributes of "Numeric String" type in the Active Directory:

1. routingNumber: This will be used to store the routing number of the bank for which the user can see the data. The routing number should be nine-digit MICR code of the bank.
2. userRole: This attribute is used to identify administrators for the bank.
    a. UserRole: WEBCHI_ADMIN.

    Note: The names of the user attributes are required to be exactly same as above.

Please refer section "Steps to configure user attributes in Active Directory" for details of how to configure the user attributes

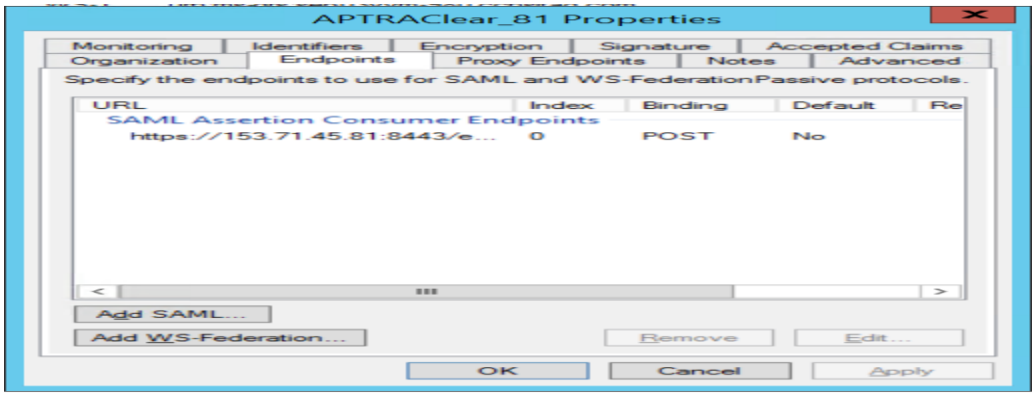
Step-2: Configuring relying party endpoint at ADFS:

Pre-requisites:

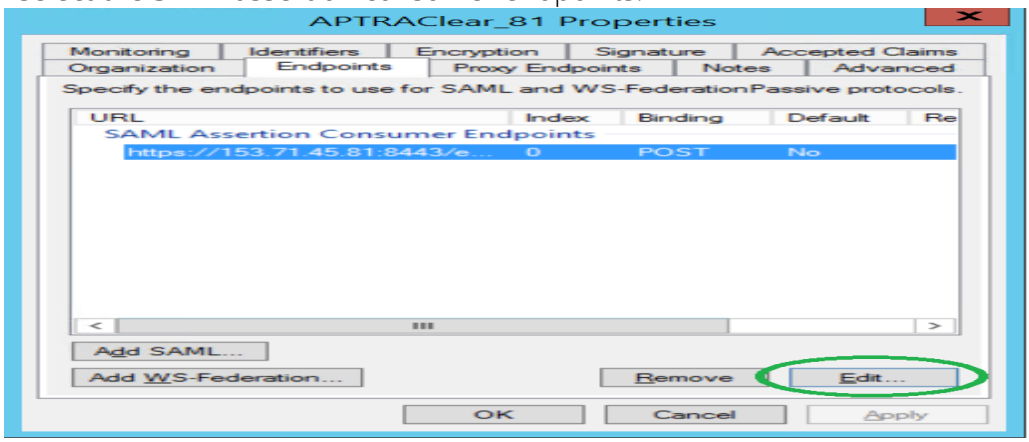
Bank is required to have ADFS role installed and configured. The ADFS role can be configured on the active directory itself or can be configured as a service on a different machine (e.g. on the DEM machine). However, it is required to have only one ADFS service active in one VLAN.

Follow below steps to configure relying party endpoint:

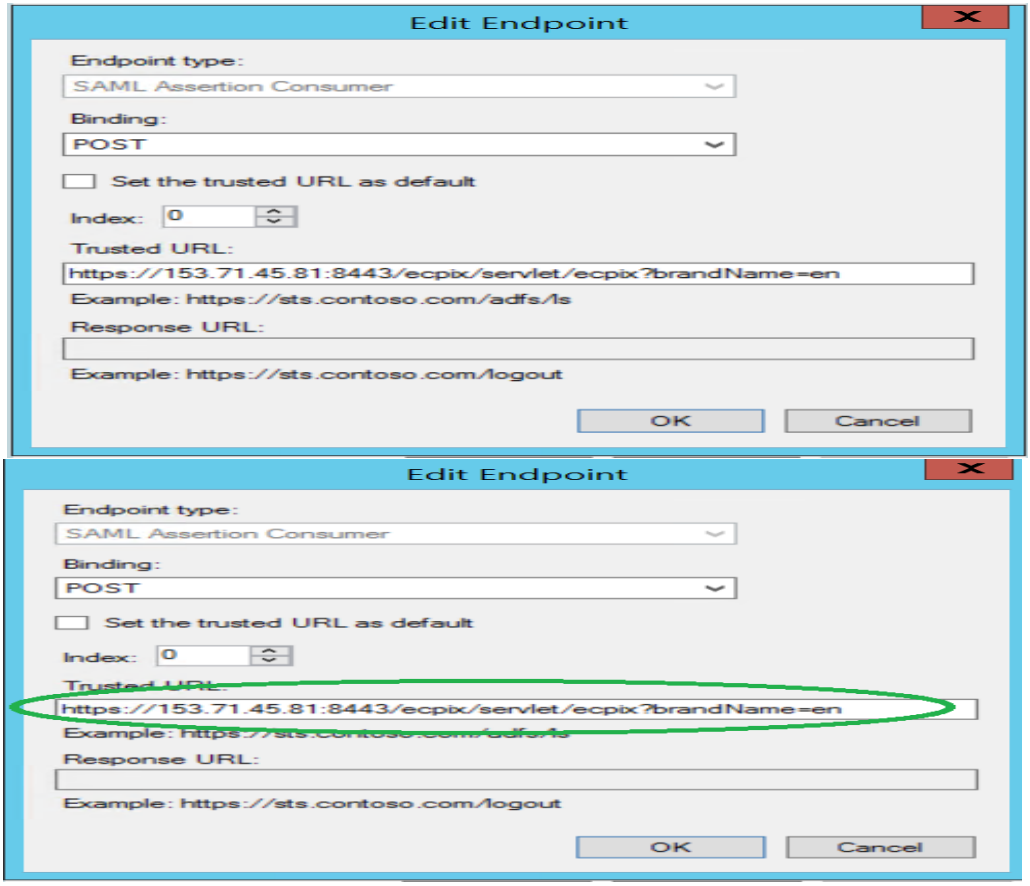
1. Navigate to ADFS Management.
2. Select relying party trusts.
3. In the middle pane, select the relying party trust created for APTRA Clear application.
4. Double Click on the relying party trust.
5. A pop-up window appears. Select endpoints Tab.



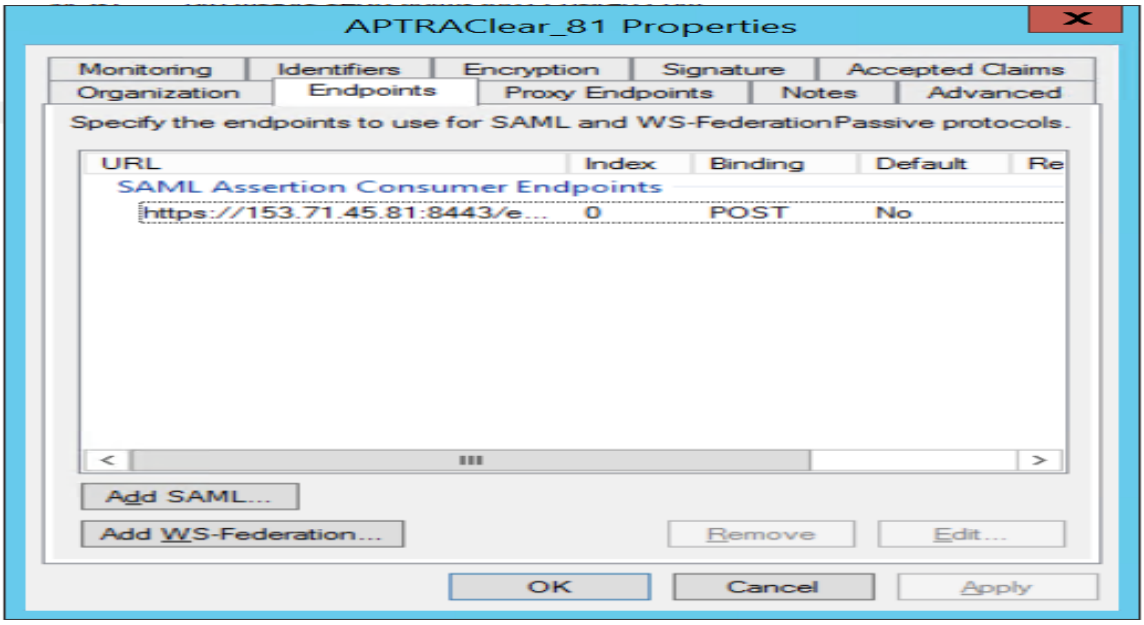
6. Now select the SAML assertion consumer endpoints.



7. Click on Edit Button.



8. Select the binding type as 'post'
9. Update the trusted URL with APTRA Clear URL which is shared by NPCI.
10. Now click on ok.



11. Click on apply.
12. Restart ADFS services.

Step-3: Configuring administrator User:

To provide administrator access to any user, following changes are required:

1. Ensure that the user is active in the active directory and can login from the machine where CCH access is required.
2. Set following user attributes for the user:

   Routing number: nine-digit MICR code for the bank

   userRole: WEBCHI_ADMIN

   Note:

   1. *The userRole attribute value is required to be exactly same as given above.*
   2. *Please refer section "Steps to configure user attributes in Active Directory" for details*

Step-4: Configuring operations users for CCH:

As a pre-requisite, bank needs to define the user roles to be permitted to access the system. E.g.: WEBCHI_OPERATOR can be used for normal operator.

After finalizing the user role name, follow steps below to configure access for the users:

3. Login to CCH UI using the WEBCHI_ADMIN user credentials
4. Define the user roles finalized as the perquisite step.

   Note: Please refer section "Steps to Configure User Groups at CCH" for details.
5. Map the screen access to a given user role.

6. Ensure that following attributes are set in active directory for all operations users:
    a. routingNumber: Nine-digit micr code for the bank
    b. userRole: Any of the user roles finalized as pre-requisite step.

Note: For detailed steps, please refer section "Steps to configure operations users in APTRA Clear as Bank Admin user"

Step-5: Configuration changes at CCH:

Before requesting configuration changes at CCH, bank must validate the ADFS configuration using following steps:

1. Open the ADFS URL in browser.

    https://[ADFS server IP]/adfs/ls/IdpInitiatedSignon.aspx
2. Select the relying party and login to the Bank AD. Once after successful login, ADFS page will be redirected to APTRA Clear URL which is shared by NPCI.
3. If URL re-direction is appearing in browser, which means AD Login is successful.
4. Banks must share above ADFS URL with NPCI to configure the bank ADFS URL in APTRA Clear. This is last step to enable the CCH access for administrator and operations users.
5. After confirmation from NPCI, bank needs to follow further steps.

Step-6: Configuring user groups at CCH:

Please refer steps detailed in c. Common Steps: Steps to Configure User Groups at CCH

Step-7: Mapping tasks to user groups at CCH:

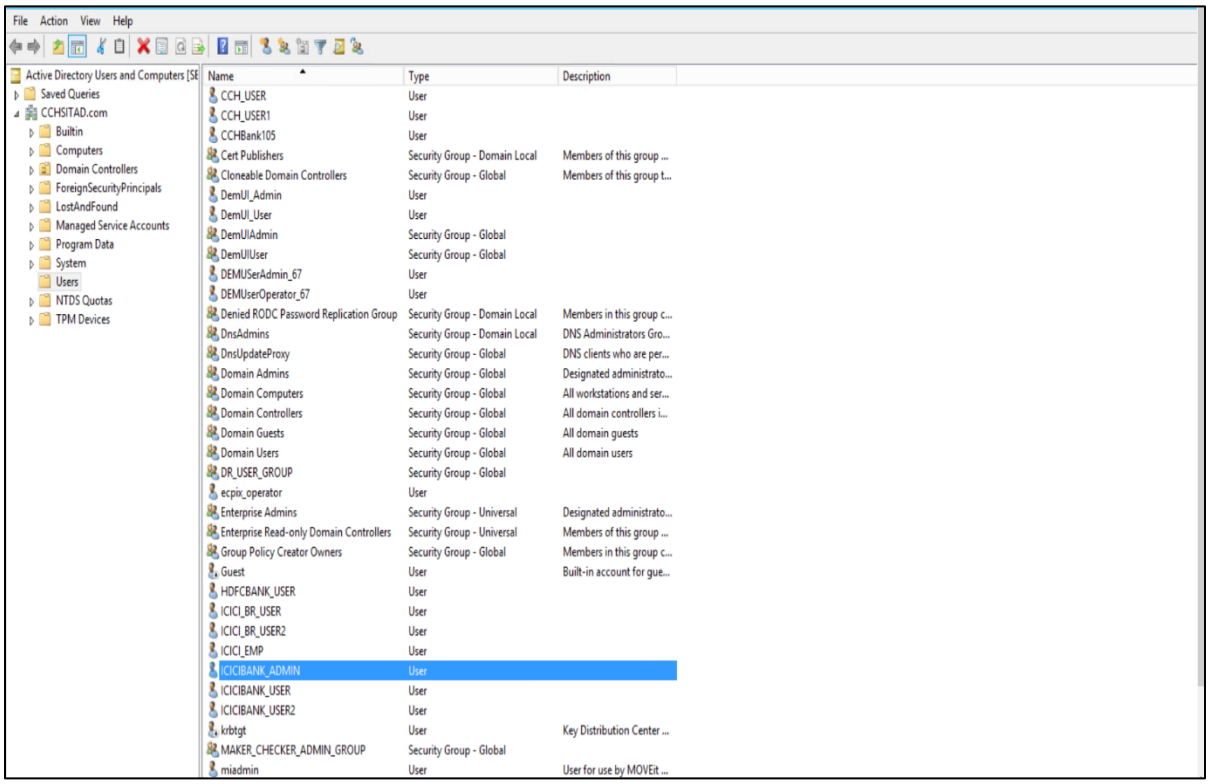
Please refer steps detailed in c. Common Steps: Steps to Map Tasks to User Groups

Step-8: Verifying bank operator login:

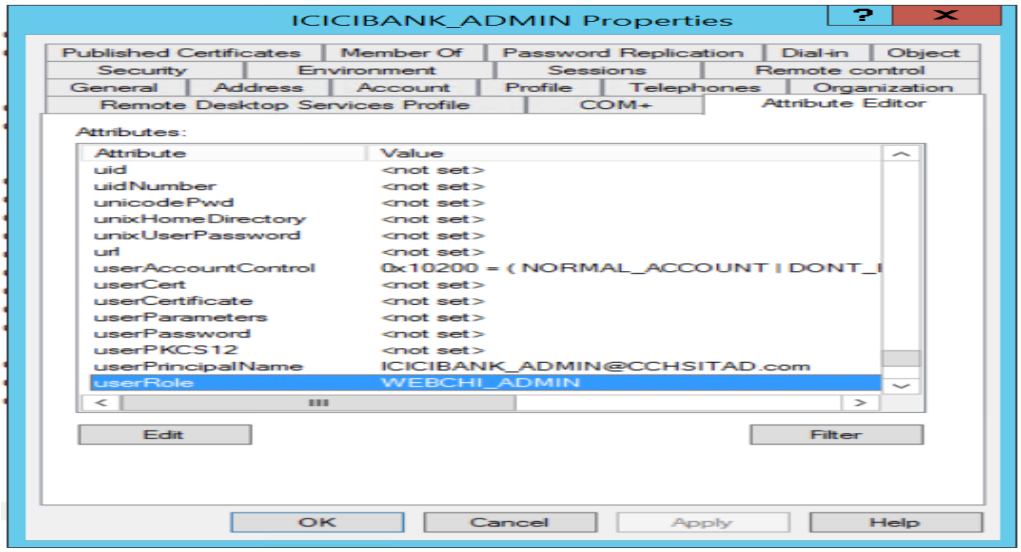
Please refer steps detailed in c. Common Steps: Steps to Verify Bank Operator Login

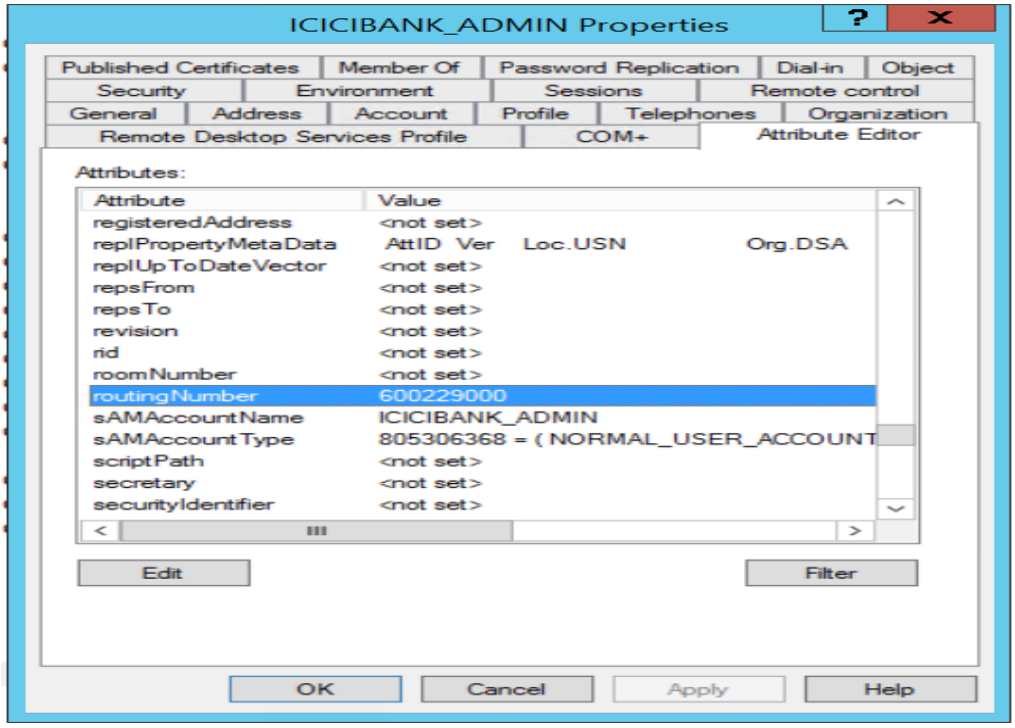
Steps to configure user attributes in Active Directory

1. Navigate to Active Directory Users and Computers.
2. Select Users in left pane.
3. Select a User and double click on it.



4. Navigate to Attribute Editor Tab.





5. Update userRole as 'WEBCHI_ADMIN' and Routing Number as 'bank routing number'.
6. Click on ok button.

c. Workgroup user & roles creation

Member banks can do the user management using Work Group, in the absence of active directory, usage of Work Group is supported. Bank has to create the users in their Work Group module and assign rights to the respective user groups to access the APTRA Clear 6.0 application

Bank must create following roles in the Work Group to map their users to enable the access to the users for the above web pages to monitor/ manage.

1. WEBCHI_ADMIN
2. WEBCHI_Operator

Step-1: Configuring administrator user:

Bank need to create WEBCHI_ADMIN group and then assign existing user to the WEBCHI_ADMIN group. This user will act as bank administrator and below mentioned steps to be followed.

a) To open Workgroup module, go to Run Dialog , enter lusrmgr.msc and press Enter
b) On the left pane click groups.
c) The system will list all the groups.
d) Click action and create new group
e) In new group specify the following details
f) group name: WEBCHI_ADMIN
g) Specify the group description
h) Members: click Add to locate and Add members in the group
i) Click create in the specified group
j) Click close in the dialog box

Step-2: Configuring operations users in Work Group:

1. In Workgroup module go to Run Dialog, type lusrmgr.msc and press Enter
2. On the left pane click groups.
3. The system will list all the groups.
4. Click action and create new group
5. In new group specify the following details
6. Group name for Ex: 'Bank_Operator'
7. Specify the group description
8. Members: click Add to locate and Add members in the group
9. Click create in the specified group
10. Repeat step 4 to 10 if you wish to configure multiple user groups (e.g. bank_operator for normal data view and bank_super_operator to view critical data)
11. Click close in the dialog box

Step-3: Configuration changes at CCH:

1. Banks must inform NPCI to configure the authentication type as 'Work Group' in APTRA Clear for the bank. This is last step to enable the CCH access for administrator and operations users.
2. After confirmation from NPCI, bank needs to follow further steps.

Step-6: Configuring user groups at CCH:

Please refer steps detailed in c. Common Steps: I. Steps to Configure User Groups at CCH

Step-7: Mapping tasks to user groups at CCH:

Please refer steps detailed in c. Common Steps: ii. Steps to Map Tasks to User Groups

Step-8: Verifying bank operator login:

Please refer steps detailed in c. Common Steps: iii. Steps to Verify Bank Operator Login

d. Common Steps:

I. Steps to configure user groups at CCH

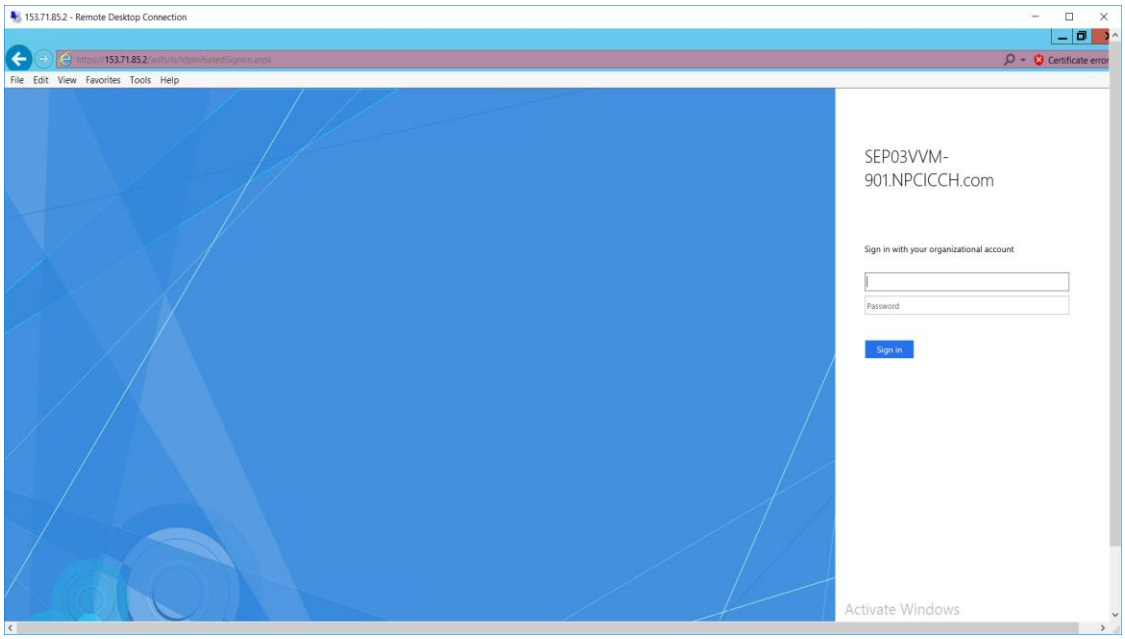
1. Open web browser and enter APTRA Clear URL.

   https://<IPADDRESS>:<Port>/ecpix/servlet/ecpix?brandName=en&routingNumber=<BankRoutingNumber>

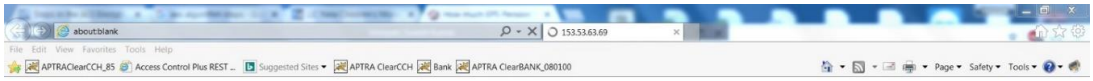
   Note: IP address will be shared through mail.

2. If bank login details are updated at CCH, following ADFS Login screen/windows credentials pop-up will appear.

   With ADFS Authentication is enabled at bank:

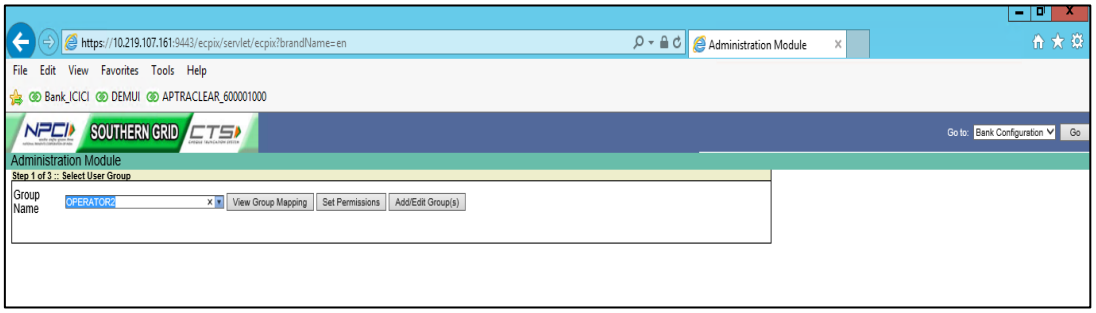


   With Windows Workgroup Authentication is enabled at bank:

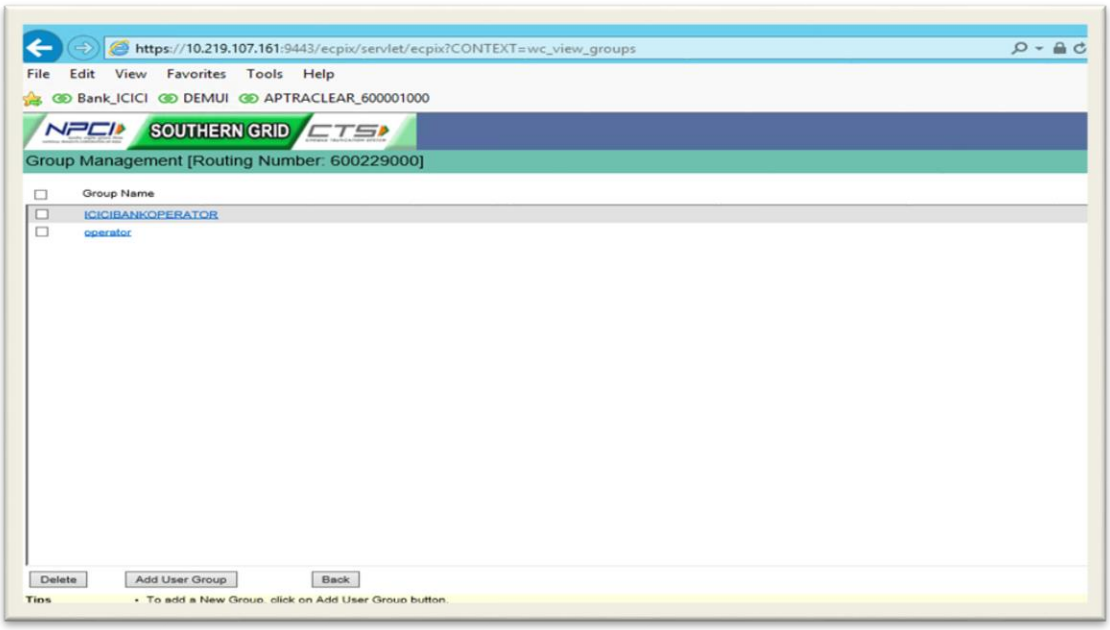


.

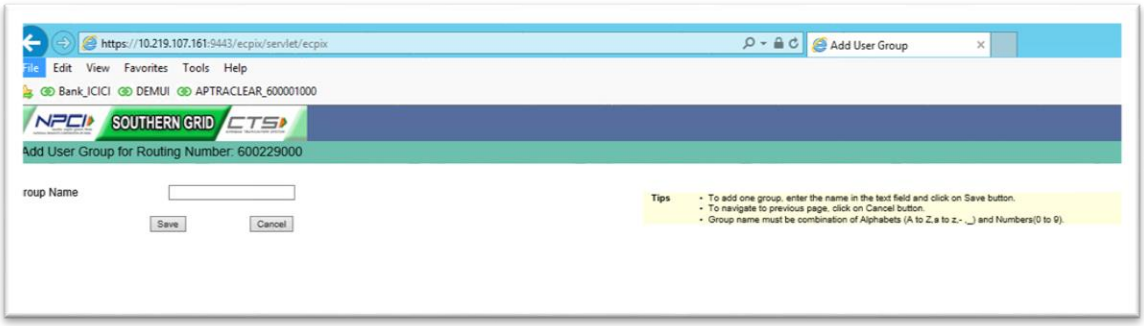
3. Please provide admin user credentials, who belongs to WEBCHI_ADMIN Group. Once after successful login, following page appears.



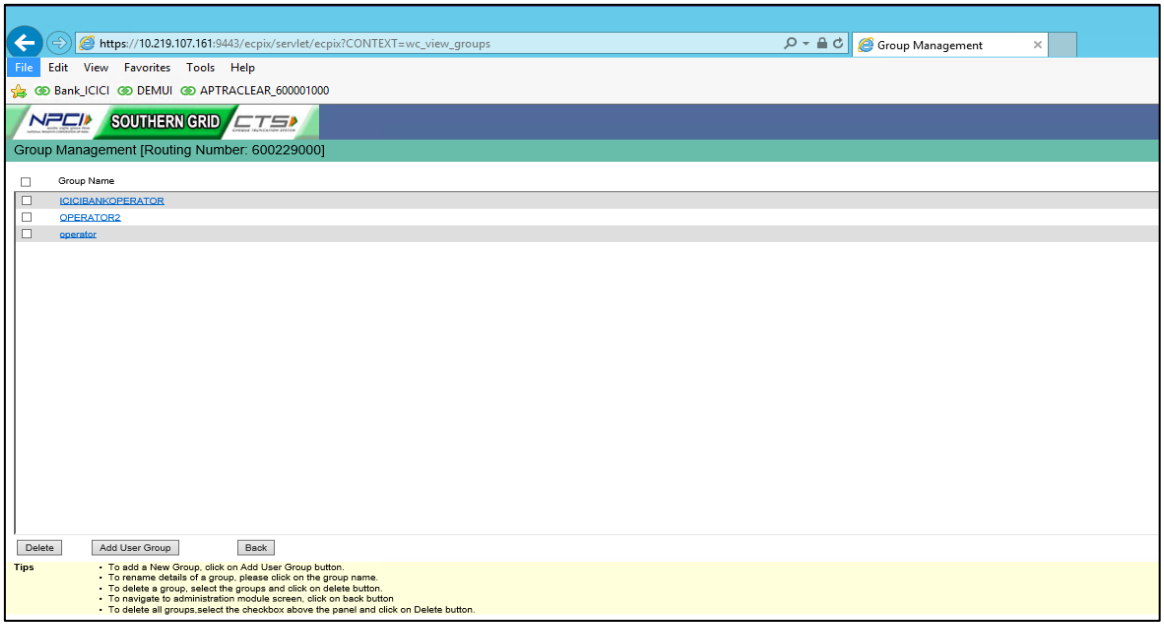
4. Bank admin user need to create different user groups using the administration module.
    a. Login using administration credentials
    b. On the administration module screen, click Add/Edit Groups.
    c. click add user group
5. Now click on add user group button to create new bank group and permission.



6. Now click on add user group button.



7. Click on save.



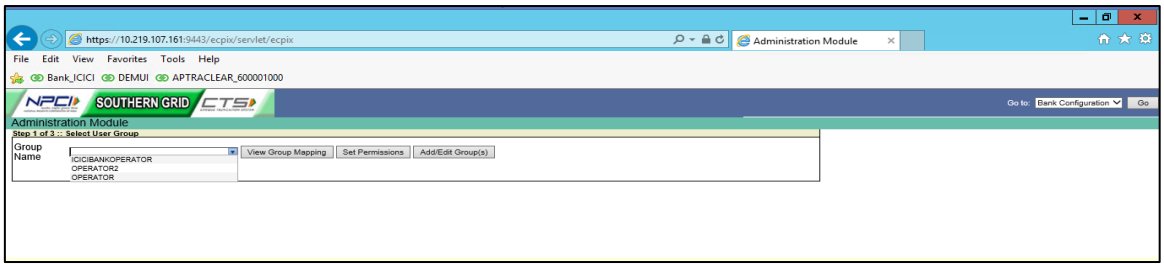
8. Now click on back button.

II. Steps to map tasks to user groups:

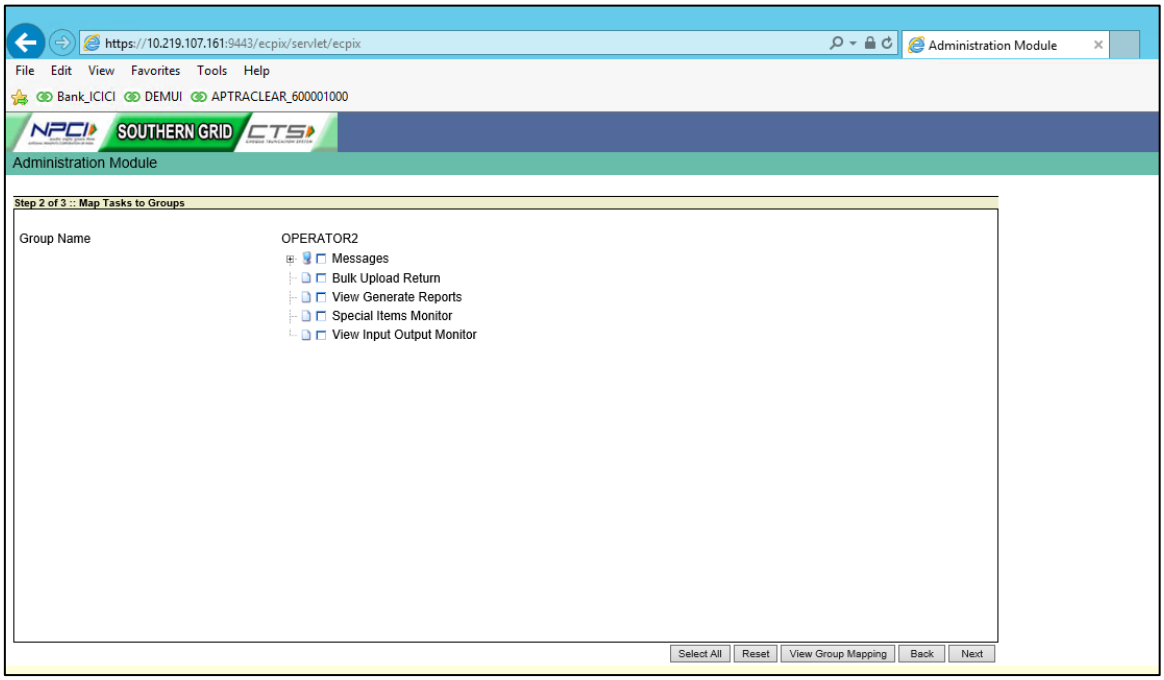
The mapping of user groups involves 3 steps:

a) Selecting user group
b) Mapping tasks to the groups
c) Confirm and save the data

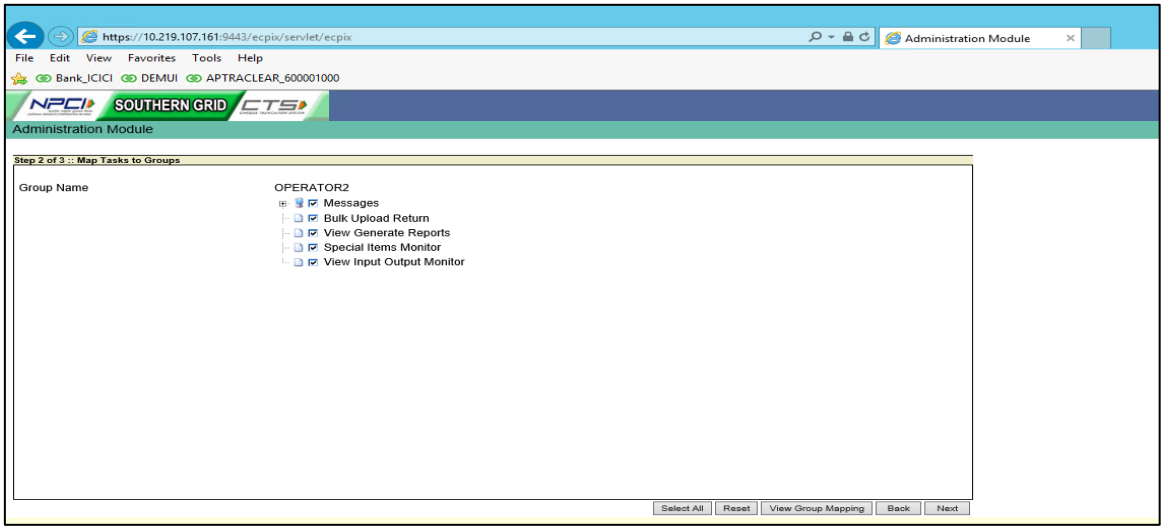
1. Select the recently created group in group name drop down.



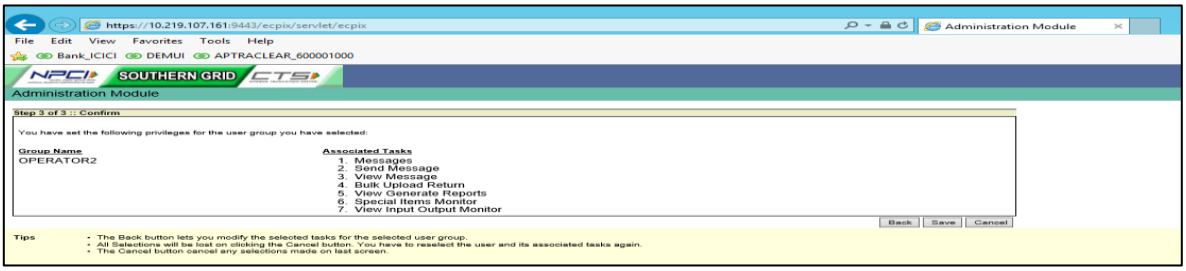
2. Click on set permissions button, then following screen will appear. The map tasks to group screen enables the mapping of user groups to available tasks.



3. Now select the tasks to the respective group.

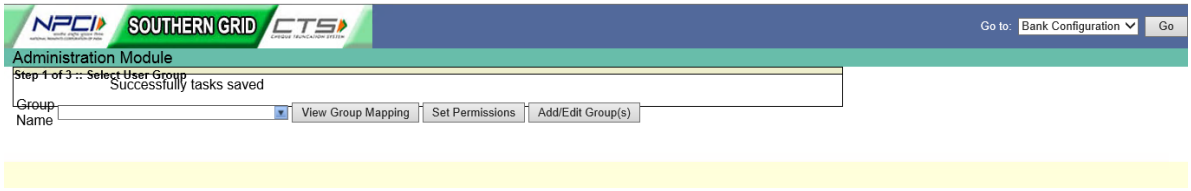


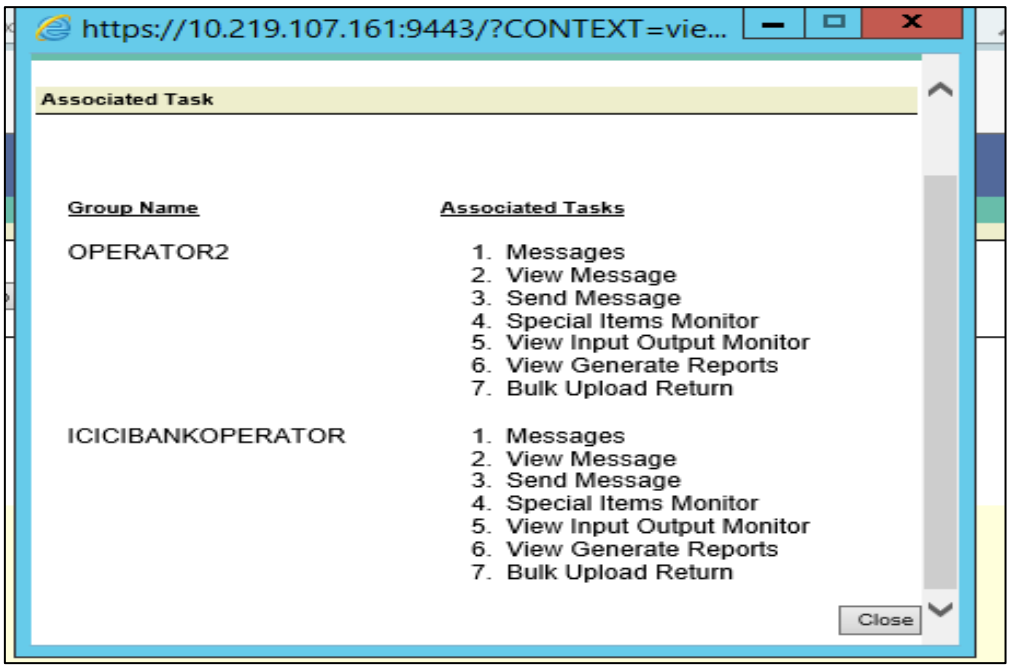
4. Click next button.



5. Now click on save.

6. Now select the role again and click on view group mapping.





7. Make sure all selected tasks associated for newly created user role 'Bank_Operator'.
8. Now, Login to Active Directory and update all users with routing number as Bank Routing Number and user role as 'Bank_Operator'.

III. Steps to verify bank operator Login:

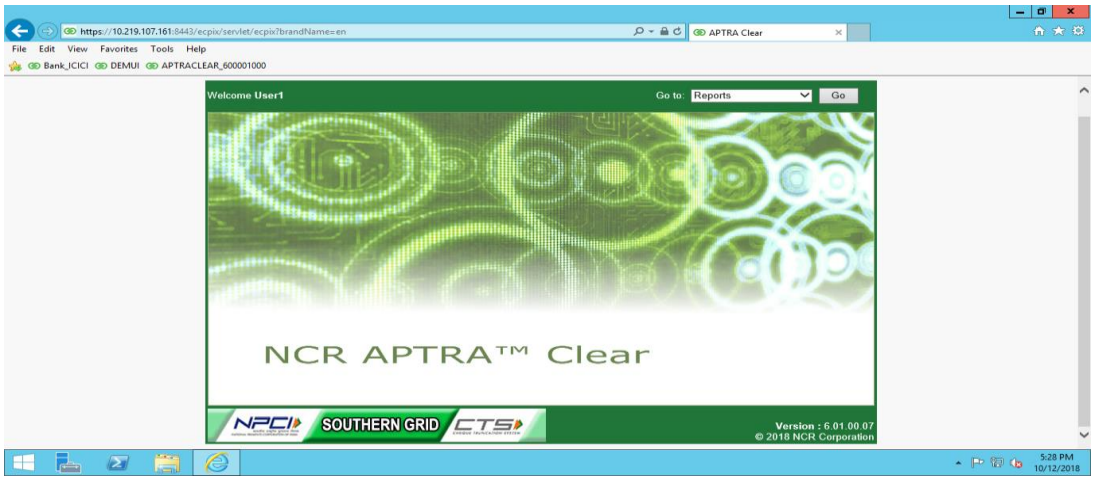
1. Open web browser and try the below URL to login to APTRA Clear as Bank user:

   https://<IPADDRESS>:<Port>/ecpix/servlet/ecpix?brandName=en&routingNumber=<BankRoutingNumber>

   Note: IP address will be shared by NPCI through mail.

2. Enter the user credentials for operations user.

   Once after successful authentication APTRA Clear bank page will be opened.



7. Summary of modifications to the previous version (1.0) of DEM specification

Revision ID	Date	Details
5	30-Sept-18	Released with clarifications and detailing of requirements. Details of individual requirements given in below table (edits/additions are in blue text)

Section	Requirement	Change
2.a.3	DEM ID: Auto generated by CTS application. It can be alphanumeric up to length 10 (VARCHAR 10)	Requirement detailed to include data type and length for DEM ID
2.b.3	Appended below screenshot: 	Requirement detailed to include sample content of signed and encrypted CIBF file
2.e.3	Naming convention for resend file is DEMID_Resend_*.txt where * can be alphanumeric string up to 35 characters.	Resend file name format changed from DEMID_Resend.txt to DEMID_Resend_*.txt
3.b.i.4	Following outward file types are required to have signing and encryption: 1. CXF 2. CIBF 3. RRF	Newly added to list file types requiring PKI security
3.b.i.5	Following outward file types does not require signing and encryption: Reconciliation file	
3.b.ii.3	Following inward file types are required to have signature verification and decryption: 1. RES	

	2. OACK 3. PXF 4. PIBF 5. RF 6. EF	
3.b.ii.4	Following inward file types does not require signature verification and decryption: 1. EOS 2. RESEND 3. SWITCHOVER 4. PDF 5. CHM	

Revision ID	Date	Details
6	10-July-19	Released with clarifications and detailing of requirements. Details of individual requirements given in below table (edits/additions are in blue text)

Section	Requirement	Change
2.b. i	Added sub section for Capture outward files	Requirement detailed to add CIIF file type for CPPS files
2.b. ii	Added sub section for CPPS outward files	
2.c. i	Added sub section for Capture Inward files	
2.c. il	Added sub section for CPPS Inward files	
3.b.i.4	CIIF outward file type is added for signing and encryption only for CPPS enabled banks.	
3.b.ii.3	CPPS_RES inward file type is added for signature verification and decryption only for CPPS enabled banks.	
3.b.i.1	Added details for Initialization vector for 3DES Padding, New line separator and Encoding method for Byte to string and vice versa	Requirement detailed to update details for PKI security.

Revision ID	Date	Details
7	4-Oct-19	Added changes for AES Encryption/Decryption algorithms.
8	10-Dec-19	Added details of AES and 3DES algorithms

Section	Requirement	Change
3.b. i	Added details for AES in outward files section	Requirement detailed to AES encryption and Description support in DEM.
3.b. ii	Added details for AES in Inward files section	
3.b.iii	Added sub section for file encryption interface.	

Revision ID	Date	Details
9	12-Feb-20	Added details for upload and download path at CCH for Bank DEM.

Section	Requirement	Change
2.a. 14	Upload and download paths added in registration of dem.	Added details for Upload and Download paths.
2.b.14	Upload path added for outward files	
2.c.9	Download path added for inward files	
6	Update the format	Formatted ADFS section

Revision ID	Date	Details
10	31-May-2020	• Updated details for. Done File and HTTP message error code 9. • Added notes to restrict files presentment of files from banks not linked to DEM • Updated context for CHM • Updated Download instructions for inward file

Section	Requirement	Change
2.b	Updated details for. Done File	DEM should not upload .Done file to CH
5	Updated Section name to Appendix-A Added HTTP Error code 9	New error code added
2.b. i	Added notes to restrict files from other banks for CXF/ RRF	File validation at Capture DEM to restrict other banks outward presentment.
2.b. ii	Added notes to restrict files from other banks for CIIF	
1.a	Updated details for CHM file	CHM details is updated in context.
2.c.20	Updated Download instructions for inward file	Updated Download instructions for inward file

Revision ID	Date	Details
11	28-Sept-20	Updated details for reports file for banks

Section	Requirement	Change
2.c. i	Updated details for report Files	Reports added in encrypted file type
2.c.16	Added note for acknowledge message	After downloading report dem bank needs to send acknowledge message.
3.b. ii.3	Updated details for report Files	Reports added in encrypted file type

Revision ID	Date	Details
12	8-Mar-21	HTTPS message added to get list of Inward files available for download.

Section	Requirement	Change
2.c.8, 2.c.9, 2.c.10, 2.c.11, 2.c.12, 2.c.13, 2.c.14,2.5.18	Add support to get Inward file list over HTTPS message for download	HTTPS message added to get list of Inward files available for download.
2.b.9, 2. c.7	HTTP failure Scenario	Updated HTTP failure Scenario
2.a.5, 2.a.6	Transcode access identifier and type is not required	Updated Access Identifier and Access type of DEM

Revision ID	Date	Details
13	13-Oct-21	Encryption and Signature Header updated

Section	Requirement	Change
3.b.i , 3.b.ii	Encoding method not specified for signature data in header.	Encoding method updated for signature header and routing number details is updated in signature and encryption header

Revision ID	Date	Details
14	26-May-23	Note added for HTTP option need to follow in case inward segregation

Section	Requirement	Change
2.c.ii.8	Inward Segregation for multiple DEM using subfolder configuration	Note added for option needs to follow in case of inward subfolder configuration for Bank.