**­**

**Functional Specifications Document**

**Cr/Dr POS Acquiring**

Version 1.10

Total Number of pages: 109

Filename: FSD\_POS Acquiring\_v1.10

Last saved: 09/03/17 17:51

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Prepared by : | Evelin Phillip | Date : | 9th February 2017 | |
|  |  |  | |  | |  |  |
| Reviewed by : | Sudarshana Mitra | Date : | 9th February 2017 | |
|  |  |  | |  | |  |  |
| Approved by : |  | Date : |  | |

**Document Distribution List**

|  |  |  |
| --- | --- | --- |
| Date | Recipient Name | Department/Division |
|  |  | Bank Business Team |
|  |  | Bank Ops & CPU Team |
|  | Jaikanth S, Deepak Culas, Hitisha Chauhan, Jimmy Karanjia, Aasim S, Suchita P | WL Business Team |
| 06-01-2017 | Rakesh Butch, Ashok Maurya, Kshitij Patil, Jayesh Damania, Vishwanath P, Ajji Gopal, Ashish Gholap | WL Technology Team |
| 09-01-2017 | Manjunath S, Vimal Fernandes, Mukesh M | WL Risk and Ops Team |

**Change History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Date | Description |
| 0.1 | Evelin Phillip | 25-10-2016 | Initial draft version |
| 0.2 | Evelin Phillip | 18-11-2016 | Added the following:   * Asset Management * Kalkulus * Terminal |
| 0.3 | Evelin Phillip | 13-12-2016 | Updated the document |
| 0.4 | Evelin Phillip | 28-12-2016 | Added the following:   * Host (Magnus) |
| 0.5 | Evelin Phillip | 04-01-2017 | Added the following:   * Clearing Settlement and Chargeback module * Risk Monitoring |
| 0.6 | Evelin Phillip | 09-01-2017 | Updated the document as per the feedback received. |
| 0.7 | Evelin Phillip | 23-01-2017 | Updated the document as per the feedback received. |
| 0.8 | Evelin Phillip | 03-02-2017 | Added the following:   * Recon Process for Rupay and Maestro |
| 0.9 | Evelin Phillip | 09-02-2017 | Added the following point –   * Bulk upload file generation in BCIF format * Addition of bank requested user input fields in insight * Mapping of Domestic Debit Card MSF * Mapping Debit Card MSF vs MCC * Pending documentation leg removed * Force settlement flag to be set default * Differential MSF process included – Phase 2 * CRN capturing leg included |
| 1.0 | Evelin Phillip | 13-02-2017 | Updated solution as per bank feedback and meeting on 8th Feb 2017 |

**Table of Contents**

[Document Distribution List 2](#_Toc474433097)

[Change History 3](#_Toc474433098)

[Table of Contents 4](#_Toc474433099)

[1. Introduction 6](#_Toc474433100)

[1.1 Purpose of Document 6](#_Toc474433101)

[1.2 Scope of Document 6](#_Toc474433102)

[1.3 Definitions, Acronyms and Abbreviations 6](#_Toc474433103)

[1.4 List of Use Cases 7](#_Toc474433104)

[1.5 Exclusions 7](#_Toc474433105)

[1.6 References 8](#_Toc474433106)

[1.7 Volume Projections 8](#_Toc474433107)

[2. SOLUTION Overview 9](#_Toc474433108)

[2.1 System Overview 9](#_Toc474433109)

[2.2 Assumptions 10](#_Toc474433110)

[2.3 Dependencies 11](#_Toc474433111)

[Functional Requirements 12](#_Toc474433112)

[2.4 Merchant On-boarding Process 12](#_Toc474433113)

[2.4.1 Use Case: UC-Insight Login-001 13](#_Toc474433114)

[UC-001: Login to the Insight Application 13](#_Toc474433115)

[2.4.2 Use Case: UC-POS-Add Merchant Details in Insight-002 15](#_Toc474433116)

[UC-002: Add Merchant details in Insight 15](#_Toc474433117)

[2.4.3 Use Case: UC-Group ME Creation-003 21](#_Toc474433118)

[UC-003: Group ME creation in Insight 21](#_Toc474433119)

[2.4.4 Use Case: UC-Risk Approval in Insight-004 23](#_Toc474433120)

[UC-004: Risk Approval in Insight 24](#_Toc474433121)

[2.4.5 Use Case: UC-NMAS/Match Approval-006 25](#_Toc474433122)

[UC-006: NMAS/Match Approval 25](#_Toc474433123)

[2.4.6 Use Case: UC-Institution ME Approval-007 26](#_Toc474433124)

[UC-007: Institution ME Approval 27](#_Toc474433125)

[2.4.7 Use Case: UC-Generation of REV, POSF & MCOM file-008 28](#_Toc474433126)

[UC-008: Generation of REV, POSF & MCOM file 28](#_Toc474433127)

[2.4.8 Use Case: UC-Installation Request Commissioning-009 30](#_Toc474433128)

[UC-009: Installation request commissioning 30](#_Toc474433129)

[2.4.9 Use Case: UC-Merchant Profile Change Request-010 32](#_Toc474433130)

[UC-010: MCR Request 32](#_Toc474433131)

[2.4.10 Use Case: UC-MCR Approval & Commissioning-011 34](#_Toc474433132)

[UC-011: MCR Approval & commissioning 34](#_Toc474433133)

[2.4.11 Use Case: UC-Parameter Change Request & Commissioning-012 36](#_Toc474433134)

[UC-012: Parameter Change request & commissioning 36](#_Toc474433135)

[2.4.12 Use Case: UC-Application Activation Request & Commissioning-013 38](#_Toc474433136)

[UC-013: Application Activation request commissioning 38](#_Toc474433137)

[2.4.13 Use Case: UC-Application Reactivation Request & Commissioning-014 40](#_Toc474433138)

[UC-014: Application Reactivation Request 40](#_Toc474433139)

[2.4.14 Use Case: UC-Application De-Activation Request-015 41](#_Toc474433140)

[UC-015: Application De-Activation Request 41](#_Toc474433141)

[2.4.15 Use Case: UC-Asset Swapping Request-016 43](#_Toc474433142)

[UC-016: Asset Swapping Request 43](#_Toc474433143)

[2.4.16 Use Case: UC-Deinstallation Request-017 44](#_Toc474433144)

[UC-017: Deinstallation Request 44](#_Toc474433145)

[2.5 Following changes to be incorporated in insight as per bank requirement **Error! Bookmark not defined.**](#_Toc474433146)

[2.6 Merchant Payment System (Kalkulus) 45](#_Toc474433147)

[2.6.1 ACCOUNTING / Fund flow for Merchant Payments 46](#_Toc474433148)

[2.6.2 Use Case: UC-Batch Processing & EOD Processing-001 49](#_Toc474433149)

[Use Case 001: Batch Processing & EOD Processing 49](#_Toc474433150)

[2.6.3 Use Case: UC-Report Generation from Kalkulus-002 53](#_Toc474433151)

[Use Case 002: Report Generation from Kalkulus 53](#_Toc474433152)

[2.6.4 Use Case: UC-Merchant Payment Advice report generation-003 55](#_Toc474433153)

[Use Case 003: Merchant Payment Advice report generation 55](#_Toc474433154)

[2.6.5 Use Case: UC-TTUM File Generation-004 57](#_Toc474433155)

[Use Case 004: TTUM File Generation 57](#_Toc474433156)

[2.6.6 Use Case: UC-Hold and Release Functionality-005 58](#_Toc474433157)

[Use Case 005: Hold and Release Functionality 58](#_Toc474433158)

[2.6.7 Use Case: UC-VIACQ Module-006 61](#_Toc474433159)

[Use Case 006: VIACQ Module report generation 61](#_Toc474433160)

[2.7 Terminal 62](#_Toc474433161)

[2.7.1 Terminal Specifications: 63](#_Toc474433162)

[2.7.2 KEY Management 64](#_Toc474433163)

[2.7.3 Application Download 64](#_Toc474433164)

[Use Case 001: Initialization 65](#_Toc474433165)

[Use Case 002: Key Exchange 66](#_Toc474433166)

[Use Case 003: Online Sale 67](#_Toc474433167)

[Use Case 004: Cash@ POS transactions 71](#_Toc474433168)

[Use Case 005: Offline Sale Transaction 74](#_Toc474433169)

[Use Case 006: Refund Transaction 77](#_Toc474433170)

[Use Case 007: Void Sale Transaction 79](#_Toc474433171)

[Use Case 008: Tip Adjust Transaction 81](#_Toc474433172)

[Use Case 009: Pre-Auth Transaction 82](#_Toc474433173)

[Use Case 010: Sale Completion Transaction 86](#_Toc474433174)

[Use Case 011: Normal Settlement 88](#_Toc474433175)

[Use Case 012: Batch Upload 90](#_Toc474433176)

[Use Case 013: Settlement after upload 90](#_Toc474433177)

[Use Case 014: Key Exchange 92](#_Toc474433178)

[Use Case 015: Online Sale 93](#_Toc474433179)

[2.8 WL Host - Magnus 96](#_Toc474433180)

[2.8.1 PORT Mapping 96](#_Toc474433181)

[2.8.2 Formats Supported 96](#_Toc474433182)

[2.8.3 Authorization Routing 96](#_Toc474433183)

[2.8.4 Data Field Definitions 96](#_Toc474433184)

[2.8.5 Online Transaction Flow for Off-us Transactions 100](#_Toc474433185)

[UC-001: Online Transaction Flow for Off-usTransaction 100](#_Toc474433186)

[2.9 Clearing Settlement and Chargeback Module - Cronus 102](#_Toc474433187)

[2.9.1 Base II Processing – Incoming 103](#_Toc474433188)

[UC-001: Base II Processing – Incoming File 103](#_Toc474433189)

[2.9.2 File Staging – Outgoing 103](#_Toc474433190)

[UC-002: File Staging – Outgoing File 103](#_Toc474433191)

[2.9.3 Chargeback process and Dispute management 104](#_Toc474433192)

[2.10 Reconciliation Process 104](#_Toc474433193)

[2.10.1 Rupay Recon Process: 105](#_Toc474433194)

[2.10.2 Maestro Reconciliation Process: 105](#_Toc474433195)

[2.11 Risk Monitoring 107](#_Toc474433196)

[2.12 Help Desk / Merchant Call Center 107](#_Toc474433197)

[3. Certifications 108](#_Toc474433198)

[4. Billing 108](#_Toc474433199)

[5. Annexure 109](#_Toc474433200)

# Introduction

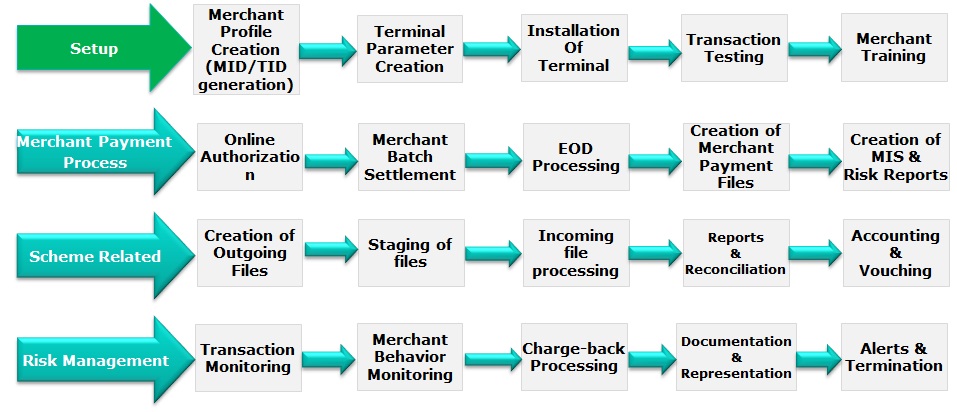
## Purpose of Document

This document describes the solution overview for offering Credit Card and Debit Card transactions Acquiring and end to end transaction processing for Bank on POS terminals.

## Scope of Document

This document outlines the scope and functional offerings for Standard POS Acquiring Solution offering, as per Bank’s agreement and requirements captured in the attached template.

The following processes shall form a part of this document.



## Definitions, Acronyms and Abbreviations

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| WL | Worldline India |
| MID | Merchant Identification Number |
| TID | Terminal Identification Number |
| POS | Point of Sale Terminal |
| PIN | Personal Identification Number used by the Card Holder to authenticate the Card Transaction at the Terminal |
| PAN | Primary Account Number is the Card Number that is identified and utilised for transaction processing by the Acquiring System |
| REV File | Terminal Parameter File downloaded from the Switch /Terminal Parameter Management System to the Terminal |
| EOD | End Of the Day |
| Scheme | Scheme is the Card Network that acts as a messenger and authorisation Body between Acquirer and Issuer Bank |
| Base I | Transaction Authorisation Leg for Card Acquiring transactions |
| Base II | Transaction Clearing and Settlement Leg for Card Acquiring transactions |
| ICTF | Issuer Centre Transmission File, provided for Onus Transactions reconciliation and matching |
| Vouching | Creation of Journal Vouchers for Reconciliation & Accounting |
| RGCS | Rupay Gross Clearing and Settlement System |
| Onus | “On-us” refers to the scenario where the issuer and acquiring banks are identical |
| Off-us | “Off-us” refers to the scenario where the issuer and acquiring banks are different |
| Magnus | Worldline Acquiring Switch |
| Insight | Merchant Automation System |
| Kalkulus | Merchant Payment System |
| TMS | Terminal Management Server |

## List of Use Cases

|  |  |
| --- | --- |
| **Use Case Name** | **Description** |
| Merchant Automation system Use Cases | Describes the various functions involved in the merchant onboarding process, asset management process, POS terminal parameters setup process. |
| Merchant Payment System Use Cases | Describes the functions involved in the file processing, data loading & validation, calculations and MIS report generation |
| Terminal Application | Describes the application setup, transaction processes. |
| WL Host | Describes the Host functions and validations for final authorization |
| Clearing Settlement and Chargeback Module | Describes the staging of outgoing files, processing of incoming files, chargeback and dispute management |

## Exclusions

|  |  |
| --- | --- |
| 1 | EMI, DCC & Dollar transactions is excluded from the scope – To be included in Phase II of POS acquiring |
| 2 | Amex Acquiring shall not be a part of this scope – To be included in Phase II of POS acquiring |
| 3 | DFS, JCB & UPI Acceptance shall not be included as a part of this Project. – To be included in Phase II of POS acquiring |
| 4 | Convenience Fee Model for transactions acquiring has been excluded from the scope – To be included in Phase II of POS acquiring |
| 6 | Cash Advance Transaction is out of scope of the project – Cash@POS is in scope by default |
| 7 | CUG card acceptance is excluded from the scope |
| 8 | Gross MDR functionality is out of scope |
| 9 | Credit card MDR template inclusion will be consider in later Phase. |
| 10 | Risk User Shall not be allowed to Edit the Input Fields by Maker or Checker. The Checker shall be able to Edit and Submit the Profile for the next workflow. |
| 11 | Billing Integration Solutions with TCH is out of scope |

## References

|  |  |
| --- | --- |
| **Document Name** | **Date** |
| Cr-DB POS -Host Message Specifications v\_13.3 |  |
| POS terminal acquiring system functional flow |  |

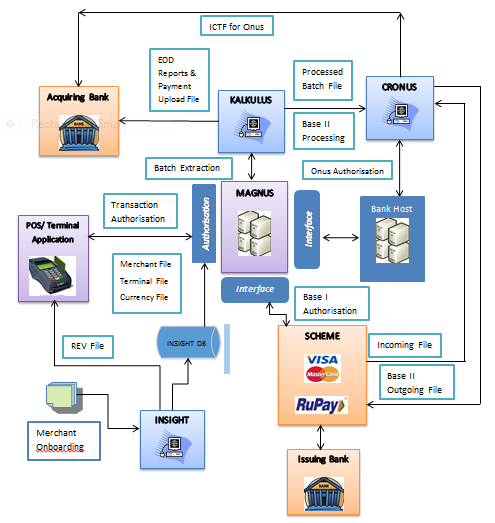
## Volume Projections

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 |
| Total Number of Terminals | NA | NA | NA | NA | NA |
| No of Acquiring transactions | NA | NA | NA | NA | NA |
| No of Users required | NA | NA | NA | NA | NA |
| Insight | NA | NA | NA | NA | NA |
| Merchant Portal / VIACQ | NA | NA | NA | NA | NA |

# SOLUTION Overview

WL India is a technology service provider for end-to-end merchant acquiring, transaction processing, merchant payments and reconciliation for various Banks.

## System Overview



The Diagram above explains the systems and High level data flow between various systems in the WL Processing Environment.

* **POS TERMINAL** - Initiates the Card Transactions
* **INSIGHT** - is the Merchant Onboarding System
* **MAGNUS** - is the WL Acquiring Switch. WL Magnus switch will be used for transaction switching to schemes and to the Bank Host (In Case of Onus transactions) for final authorization.
* The Integration with Magnus Interface with Banks’ Switch shall be done basis the WL External Host Message specifications format. And the ICTF shall be shared with the Acquiring Bank for the same for the transaction matching and posting on the Issuer side. Formats shared in the Annexures.
* **KALKULUS** - is the Merchant payment system which performs the Batch Processing and Merchant payment processing at EOD.
* **CRONUS** - is the Clearing and Settlement System which performs the Staging of Files and Incoming Files. It also performs the Chargeback and Dispute Management Function.
* Ownership of the POS terminal device shall be with WL. End-to-end Field Services and Logistics for the terminals will be handled completely by Worldline FSD Team.
* WL will support bank for doing end to end merchant acquiring and respective merchant support will be given by WL; the support would include terminal procurement, leasing, installation and maintenance.
* Transaction processing from POS terminal shall be the responsibility of WL.

## Assumptions

|  |  |
| --- | --- |
| 1 | The Insight workflow as per the given use cases is as per Multibank offering; It contains feasible bank requested changes. |
| 2 | Merchant Payment system consists of EOD processing in the Kalkulus module |
| 3 | The document covers only basic Credit/Debit POS transaction flow. There shall be a separate document for NFC acquiring. (refer [Annexure P](#_Annexure_1)) |
| 4 | The document does not include any aggregator workflow with respect to transaction routing. |
| 5 | The document does not include the implementation of any additional ad-hoc government initiatives or customizations in settlement and payment process. However existing Govt mandate implemented will be in effect. |
| 6 | Cashback transactions are allowed for certain MCC, for some specific MCCs the scheme restricts the transaction. |
| 7 | Any introduction of a new transaction type to be accepted at the POS terminal shall require certification with the scheme. Please refer details in section 3 for the same. |
| 8 | In case of an expired kernel of a terminal, a new certification shall be required for any change to be implemented at the POS terminal. |
| 10 | Debit card MSF will be default populated for all MCC’s all merchants discussed with the bank as per existing Govt mandates. |
| 11 | Group ME creation workflow will be utilised by Bank Bank in later phase. |
| 12 | Institution approval will be utilised by Bank bank in later phase. |
| 13 | Offline Sale, Key Entry, pre-auth cases will be only allowed in cases where Bank Risk Team approves. Refund transactions shall be disabled for all Bank Merchants.  Can be managed through Insight under application parameter through the approver workflow. |
| 14 | TIP transactions shall be allowed up till the CAPED value captured at the time of on-boarding. |
| 15 | For Non Bank / New Customer for Bank, the Bank will use ME Bulk Upload Workflow only. |

## Dependencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr No** | **Dependency** | **Responsibility** | **Date of Closure** | **Status** |
|  |  |  |  | **Open** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Functional Requirements

## Merchant On-boarding Process

Merchant creation will be done in WL Merchant Onboarding Module - Insight.

Insight is used to manage merchant setup, work flow with respect to the Merchant / Terminal Installation/De-installation, POS terminal Parameter management, and Asset management in WL systems.

**Key Features of Insight: -**

* Merchant setup process would be initiated and managed through Insight.
* The Bank shall process files through Insight Screen, wherein the user shall be a Maker and there shall be an Admin User for Approval / Deletion of request raised.
* For all Merchants on-boarded, VISA/ MasterCard / Maestro / RuPay acceptance shall be default enabled for the banks. ***Going forward Amex and Internationals schemes routed through Rupay will be enabled as and when certification process completed with KMBL.***
* Provision will be provided to capture whether a merchant can accept domestic or international cards or both. By default it should be All Cards Acceptance.
* All the data captured in Insight should be passed to WL transaction processing, settlement and clearing system.
* Bank will be on-boarding the merchant in Insight through the Web UI access (to be provided by WL). Provided below are the sample screen shots of the Insight Screens available to the Web User.(see [Annexure C](#_Annexure))

Merchant Onboarding

Fig. Merchant Automation System

### Use Case: UC-Insight Login-001

Insight Login (1)

|  |  |  |  |
| --- | --- | --- | --- |
| UC-001: Login to the Insight Application | | | |
| **Description** | | This use case describes the process for an existing user to login to the Insight application | |
| **Actors** | | Bank, Insight | |
| **Pre-Condition** | | 1. Bank should have the Insight URL which is shared by the WL team 2. Whitelisting of Bank proxy IP address – Insight to be accessed from Bank’s network only 3. Bank should be pre-registered to the Insight application 4. Bank should have login credentials shared by the WL team for logging into the Insight application | |
| **Post-Condition** | | 1. Bank should be able to login successfully to the Insight application 2. Post login, Bank should be able to view the menu options from the homepage of the Insight screen | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | Bank user enters the Insight URL on the web browser of his system | | The Insight Login screen opens on the web browser |
|  | Bank user views the login screen on his web browser | |  |
|  | Bank user enters the login credentials on the Insight application | | The Insight system captures the entered user credentials and validates the same from the backend. |
|  | Bank user views the Insight menu options once he is successfully logged into the Insight system | |  |
| **Alternate Flow** | | | |
| **Step** | **Scenario** | | **User/System Action** |
|  | User forgets his username/password | | User can click on the ‘Forgot Password’ option to retrieve his password. |
| **Business Rules** | | | |
|  | There are four users for the Insight login:   1. Bank Onboarding Maker – data entry as well as bulk upload -> Bank CPC Maker, Bank BSG User (Entry for Specific Masters) 2. Bank Onboarding Checker - data entry as well as bulk upload 3. WL Field Service user 4. Risk User -> Bank Credit Risk Checker, 5. Bank Audit User, Bank BSG User – View Rights for all Workflows | | |
|  | Bank should be pre-registered to the Insight application and the credentials should be shared by the WL team to the respective bank | | |
|  | Password shall be reset as triggered by WL on User notification. | | |
|  | User Id and Password shall be as per WL security policy. | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | User enters incorrect Username & Password combination | | Appropriate error message will be displayed to user stating that the entered credentials are not incorrect. |
|  | User doesn’t enters username or password and clicks on the Submit button | | Appropriate message will be displayed to user stating that the required fields are mandatory |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired |

### Use Case: UC-POS-Add Merchant Details in Insight-002

ME creation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| UC-002: Add Merchant details in Insight | | | | |
| **Description** | | This use case describes the merchant onboarding process through the Insight system in two ways:   1. Entering the new ME details into the Insight screen 2. Uploading the Merchant bulk onboarding file in the Insight | | |
| **Actors** | | Bank, Insight | | |
| **Pre-Condition** | | The Bank should have all the Merchant related information as per the WL specific Merchant Parameters as defined in [Annexure A](FSD_POS%20Acquiring_v0.8.doc) | | |
| **Post-Condition** | | 1. Insight will be generating MID post all the Approval Workflows and will be pushed to the next workflow. 2. The Maker shall Save the input fields. All the Mandatory Fields to be input and then only he can save the fields. The Checker shall Submit the Input Fields after Review, in case he rejects the entry, it shall show under Pending for Submission workflow under his Login. 3. ME profile is created in Insight | | |
| **Main Flow** | | | | |
| **Step** | **User Action** | | | **System Action** |
|  | Bank user will be logging into the Insight system using his username and password | | | The Insight system captures the entered user credentials and validates the same from the backend. |
|  | Bank user to go in to Existing Merchant Workflow or to New Merchant Workflow.  There shall be a separate flag for identifiying this selection. | | | System will auto populate the CRN and Account Number from the Bank Master in case of New Merchant Input through Insight Screen ; Bulk upload flow shall include the CRN and Account Number during input. |
|  | **Add ME Profile:**  Bank user will select the Masters🡪Add ME Profile to add a new merchant  Bank user will input all details with the various input parameters through fields provided such as -   * Application ID – User to input barcode no as per Bank process. * Customer ID (existing Merchant to input CRN, New merchant CRN to be system populated ) * Merchant Type * Merchant Details * Branch Details * Merchant Address * MCC and TCC code * Mailing Address * Principle Owner Details * Principal Owner PAN ( Mandatory field) * Other Merchant Details * Daily and Monthly Transaction limit * Per transaction limit * Document Checklist * Configure Domestic Debit/Differential MSF * EDC Installation Request Details * Application Details * Establishment Year * Registration No * Registration effective date * RM Code * LG Code * LC Code * Firm PAN * NEW\_OLD Flag   Bank user will be able to save the ME details by clicking on the “Save” button | | | System will prompt for a predefined error as per the logic set in the given field.  If all the entered fields are correct, then Insight generates the MID and TID for that merchant  CRN to be prepopulated each time whenever new merchant is created.  CRN to be picked from bank Master.  Bank shall also provide the Account Number Dump that will be allocated to the CRN which has been provided by the Bank for a New Customer Creation. |
|  | **Following new input fields to be added in phase II**   1. **Charging parameters to be confirmed by the Bank.**   **Eg. Low throughput charges**   1. **Volume parameters to be confirmed by the Bank.**   **Eg. Minimum throughput, Merchant turn over categorywise** | | |  |
|  | Bank checker user has to access the pending For Submission request. | | | The ME profile is created in the Insight database and ME request will log under ‘’Pending For Submission’’ queue |
|  | Bank checker USER will verify the ME profile/ make the correction if any and Submits the profile. | | | ME request will push forward for further approval stages. |
| **Alternate Flow** | | | | |
| **Step** | **User Action** | | | **System Action** |
|  | **Bulk ME Onboarding workflow:**   1. Bank user will go to the “Asset Management” option from the Insight screen. 2. Select the “Bulk Request Upload” option to upload the bulk ME file 3. Bank user follows the below steps to upload the file:  * Select Institution(dropdown) * Select Request Type(dropdown) * Select file to upload(browse file to upload)  1. Bank user uploads the Bulk Onboarding format file with mandatory fields filled into Insight (see [Annexure A](#_Annexure)) | | | * The system processes the Bulk Onboarding file and creates a Log file (see [Annexure B](#_Annexure)) * The log file includes the details of each line entry with a success or failure status * The Bulk Success log file with MIDs genrerated and push to next workflow. |
|  | Bank user reviews the log file for success or rejection and re-uploads the rejected entries with the correction | | | For Successful entries, the status is Y and status is N for rejection.  Rejected status is updated with reason of rejection |
|  | **Bulk Merchant Approval:**   1. Bank Checker user will go to the “Asset Management” option from the Insight screen 2. Select the “Bulk Merchant Approval” option to approve the bulk onboarded merchants 3. Bank user will search the ME records by following the below steps:  * Enter the From and To date * Enter the File name * Enter the Request ID * Select the Status  1. Bank user will select the record(s) and perform any of the following options:  * Submit * “Save” option will save the selected records. * “Reject” option will reject the selected records and the user will enter the reason for rejection. | | | The “Bulk Merchant Approval” screen is displayed on the Insight screen   * The system displays the searched records * The system displays the message “Merchant Saved Successfully” in the case of saving a record * The system displays the message “Merchant Submitted Successfully” in case of approving a record * The system displays the message “Request Rejected Successfully” in case of rejecting a record * The system prompts an error message “Enter reason for rejection” if the user hasn’t mentioned any reason in the case of rejecting a record. * TID shall be generated after risk approval and MATCH/TRACE approval. |
| **Business Rules** | | | | |
|  | Each Merchant will have a single MID and can have multiple TIDs as per the number of terminals installed | | | |
|  | MID will be a 15 digit number and TID will be 8 digit Number | | | |
|  | MID Logic will be as follows:   |  |  | | --- | --- | | BANK CODE | Two digits | | ZONE CODE | Three digits | | BRANCH CODE | Five digits | | BRANCH SERIAL | Four digits |   Bank Code will be zero padded.  Branch code should have only numeric logic as defined in WL system.  For online merchant on-boarding the MID logic will be system generated predefined logic where in merchants will be allocated sequential no. WL to ensure that the MID generation shall not be restrictive for Online Merchant Generation through Insight. | | | |
|  | TID Logic will be as follows:  This logic is WL system generated logic and its based on internal system mapping.  The MID and TID combination for each merchant shall be Unique. However, TID can be duplicate across Merchants.   |  |  | | --- | --- | | Payment City CODE | Two digits | | Bank code | Two digits | | Sequence No. | Four digits | | | | |
|  | MSF Structure shall be defined for each merchant creation as follows:   |  |  | | --- | --- | | **Domestic Debit Cards (default)** | | | Up to Rs 1000 | 0.25% plus taxes | | Rs 1001 to Rs 2000 | 0.5% plus taxes | | Rs 2001 and Above | 1% plus taxes |  |  | | --- | | Debit MSF 0 to 1K | | Debit MSF 1001 to 2K | | Debit MSF% > 2K | | Credit MSF MC% | | Credit MSF VISA% | | Credit MSF RuPAY% | | | | |
|  | Differential MSF matrix shall be available for Bank Merchant please refer Annexure R | | | |
|  | Fuel surcharge for Domestic MasterCard and Visa Debit cards is as follows:   |  |  | | --- | --- | | **Domestic Debit Cards** | | | 0 to 2 K | 0.75% plus taxes | | Rs 2001 and Above | 1% plus taxes |   The surcharge on **credit card transactions** will be Rs.10 or 2.5% of transaction amount whichever is higher . | | | |
|  | Merchant Account number should be equal to 15 digits – This fields corresponds to Merchant settlement account number. This also applies to beneficiary account no field for NEFT merchant. | | | |
|  | Branch SOL ID should be 5 digits number. This refers to the bank branch code. | | | |
|  | Bank user can upload a bulk ME file through the Masters option from the Insight screen. System will display the “Bulk Request Upload” option when logged in as a Bank user. | | | |
|  | The ME Bulk upload file should have a name convention of the format *<<BanknameME-CurrentDate-serial no>>.*  The file name has duplicate validation check in Insight, special characters not allowed as per PCI guidelines. | | | |
|  | Merchant and Firm PAN to be mandatory field | | | |
|  | Insight will support to MS excel 2010 and 2013 format where there is no limit of no of fields to be supported. | | | |
|  | Merchant classification to be selected ‘’Retail’’ as default. | | | |
|  | Following Insight Masters to be utilized. WL to share the same with Bank Bank  MCC code  TCC code  Location – state – city mapping  Pincode | | | |
|  | Authorization and Force settlement application parameter to be set as default enabled. | | | |
|  | Approved by field need to be make Non –Mandatory. | | | |
|  | Bank to add branch and Zone details to create Master in Insight. | | | |
|  | Asset Owner for every Bank merchant should set default as Bank | | | |
|  | Trace clearance flag to be set as default Deselected. | | | |
|  | There is currently no IFSC Code validation for IFSC input for both Bank and non-Bank Customer | | | |
|  | For every Merchant Request, only one Terminal Type can be selected and multiple terminals for a request. For multiple terminal types, there shall be separate Additional Terminal Request workflow to be utilized. | | | |
|  | Only New customers to be pushed into the BCIF file at EOD as per format shared by the Bank, based on the NEW\_OLD flag | | | |
| **Exceptional Flow** | | | | |
| **Sr. No.** | **Exception** | | **Error Message** | |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired | |
|  | A merchant being created with the same account number as one already in the system | | System prompts a message “A merchant exists with MID with the given account Number” | |
|  | Name of the merchant entered with special character | | System Prompts “Special Characters not allowed for Merchant Name” | |
|  | Account number entered less than 15 digits for Bank or Non Bank customer. | | System prompts “Merchant account number should be 15 digits” | |
|  | Merchant enters alphanumeric characters | | System prompts “ Alphanumeric characters not allowed” | |
|  | A merchant being created with the already used Application no. | | System prompts a message “Application number already exists” | |
|  | A merchant being created with the already used CRN number. | | System prompts a message “CRN number already exists” | |
|  | A merchant being created with the already used LMS ID | | System prompts a message “LMS ID already exists, Please provide a different LMS ID.” | |
|  | ME Bulk file uploaded in incorrect format | | System prompts a message “Invalid file name convention. Please upload file name with proper format” | |
|  | Merchant Legal name is not entered | | System prompts a message “Enter Merchant Legal name” | |
|  | Merchant DBA name is not entered | | System prompts a message “Enter Merchant DBA name” | |

### Use Case: UC-Group ME Creation-003

**Group ME**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| UC-003: Group ME creation in Insight | | | | |
| **Description** | | This use case describes the group ME creation workflow in Insight | | |
| **Actors** | | Bank, Insight | | |
| **Pre-Condition** | | The Bank has all the Merchant related information as per the WL specific Merchant Parameters | | |
| **Post-Condition** | | 1. Bank user will be having the pre generated group MID as per logic provided in the System 2. Group ME profile is created in Insight | | |
| **Main Flow** | | | | |
| **Step** | **User Action** | | | **System Action** |
|  | Bank user will be logging into the Insight system using his username and password | | | The Insight system captures the entered user credentials and validates the same from the backend. |
|  | 1. Bank user will select the Masters🡪Merchant Group Profile🡪Add Merchant Group Profile to add a new group merchant 2. Bank user will input all details with the various input parameters through fields provided such as -  * Merchant Name * Merchant Details * Branch Details * Merchant Address * MCC and TCC code * Mailing Address * Principle Owner Address * Other Merchant Details * Document Checklist  1. Bank user will be able to submit the ME details by clicking on the “Submit” button | | | * System will prompt for a predefined error as per the logic set in the given field. * If all the entered fields are correct, then Insight generates a Group ME code for that merchant |
| **Alternate Flow** | | | | |
| **Step** | **User Action** | | | **System Action** |
|  | NA | | | NA |
| **Business Rules** | | | | |
|  | MID will be a 15 digit number | | | |
|  | MID Logic will be as follows:   |  |  | | --- | --- | | BANK CODE | Two digits | | ZONE CODE | Three digits | | BRANCH CODE | Five digits | | BRANCH SERIAL | Four digits |   Bank Code will be zero padded  Branch code should have only numeric logic as defined in WL system. | | | |
|  | MSF Structure shall be defined for each merchant creation as follows:   |  | | --- | | Debit MSF% <= 2K | | Debit MSF% > 2K | | Credit MSF MC% | | Credit MSF VISA% | | | | |
|  | Fuel surcharge for Domestic MasterCard and Visa Debit cards is as follows:   |  |  | | --- | --- | | **Domestic Debit Cards** | | | Up to Rs 1000 | 0.25% plus taxes | | Rs 1001 to Rs 2000 | 0.5% plus taxes | | Rs 2001 and Above | 1% plus taxes |   The surcharge on **credit card transactions** will be Rs.10 or 2.5% of transaction amount whichever is higher | | | |
|  | Merchant Account number should be equal to 15 digits | | | |
|  | Branch Sole ID should be 5 digits number | | | |
|  | Application Number should be alphanumeric characters with alphabets as upper case | | | |
| **Exceptional Flow** | | | | |
| **Sr. No.** | **Exception** | | **Error Message** | |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired | |
|  | A merchant being created with the same account number as one already in the system | | System prompts a message “A merchant exists with MID with the given account Number” | |
|  | Name of the merchant entered with special character | | System Prompts “Special Characters not allowed for Merchant Name” | |
|  | Account number entered less than 16 digits | | System prompts “Merchant account number should be 16 digits” | |
|  | Merchant enters alphanumeric characters | | System prompts “ Alphanumeric characters not allowed” | |
|  | A merchant being created with the already used Application no. | | System prompts a message “Application number already exists” | |
|  | A merchant being created with the already used LMS ID | | System prompts a message “LMS ID already exists, Please provide a different LMS ID.” | |

### Use Case: UC-Risk Approval in Insight-004

Pending Risk Approval (2)

|  |  |  |  |
| --- | --- | --- | --- |
| UC-004: Risk Approval in Insight | | | |
| **Description** | | This use case describes the risk approval flow in the Insight system | |
| **Actors** | | Bank, Insight | |
| **Pre-Condition** | | ME profile created with Risk Approval selected as Yes | |
| **Post-Condition** | | 1. Merchant record(s) is risk approved 2. Insight database is updated after the approval | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
| 1 | Bank user will be logging into the Insight system using his username and password | | The Insight system captures the entered user credentials and validates the same from the backend. |
| 2 | **Risk Approval:**   1. Bank user will select Approval🡪 Pending Risk Approval link from the Insight screen 2. Bank user will be able to search the merchant record pending for risk approval using the Merchant Code or user can also view all the records by selecting the “Display All” option 3. Bank user will be able to approve a merchant record pending for risk approval by selecting the record and clicking on “Approve” 4. Bank user can also enter the Risk Approval remark if any and then approve the record(s) 5. Once MID Creation happens on basis of data entry by Maker / Checker, data is sent Parallely to 2 places. First for MATCH / NMAS & 2nd to risk approver. 6. Only if positive response comes from both sources ie.. Risk Approver and NMAS / MATCH approval, then only TID will be created. 7. In case of negative response from Risk approver & positive response from NMAS / MATCH, TID will not be created. | | * The “Risk Approval Pending” screen is displayed on the Insight screen * The Insight screen will display all the records whose Risk Approval is pending * The Insight screen will ask confirmation and on confirming, display Bulk Risk Approved successfully |
|  |  | | Insight database is updated after the approval. |
| 3 | In event of risk decline cases, it will be log under ‘’Risk Decline ME profile’’ | |  |
| 4 | Risk USER can access ‘’Special Risk Approval Tab’’ to approve Risk / Match –NMAS decline cases on exception basis. | |  |
| **Business Rules** | | | |
| 1 | Requirement of Risk approval for all merchant record shall be default ‘’YES’’. It is mandatorily ‘’YES’’ for all Offline Bank Merchant onboarding.  For Online Merchant Onboarding, this shall be Default “ NO”. | | |
| 2 | Bank shall maintain the Risk Comments for Decline and Approval for Records for the Onboarding process, as a Screenshot or Physical Printout on the Bank’s end. | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired |
|  | User tries to enter an incorrect ME code (Referred as MID) | | Appropriate error message will be displayed to the user that no such record was found |
|  | User tries to enter incorrect ME Name | | Appropriate error message will be displayed to the user that no such record was found |

### Use Case: UC-NMAS/Match Approval-006

NMAS-Match Approval

|  |  |  |  |
| --- | --- | --- | --- |
| UC-006: NMAS/Match Approval | | | |
| **Description** | | This use case describes the NMAS/Match approval flow | |
| **Actors** | | Worldline Insight User, Insight | |
| **Pre-Condition** | | 1. The Match File will be uploaded by WL and Response shall be downloaded. 2. Bank to check the response and accordingly approve or reject the merchant onboarding based on Match response. 3. New ME profile uploaded and submitted successfully 4. ME profile created with NMAS/MATCH approval selection | |
| **Post-Condition** | | Merchant profile(s) is NMAS/Match Approved | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | User will be logging into the Insight Global using his username and password | | The System captures the entered user credentials and validates the same from the backend. |
|  | User will select the NMAS/Match Clearance Approval link from the Insight screen | | The “NMAS/Match Clearance Approval” screen is displayed on the Insight screen |
|  | User will select the “Institution” from the dropdown and select the Bank  User will enter Merchant Code and search the record. | | The Insight screen will display the merchant record(s) the user searched for |
|  | User will select the NMAS/Match checkboxes and click on the Approve button | | The Insight screen should ask confirmation and on confirming, display Bulk NMAS/MATCH Approved successfully |
| **Business Rules** | | | |
|  | For New merchant enrolment Match functionality is available with WL. The details of the new onboarded merchants are sent in batches to the Master Card as a manual process by 5.30 pm on the day of Onboarding request and response is received next day morning. The Match File will be uploaded by WL and Response shall be downloaded. However, the final decision will be taken by the Bank. Bank will check the response and accordingly approve or reject the merchant onboarding based on Match response. | | |
|  | If the user checks the Post-Facto Trace/match option while creating new ME profile, then Workflow will proceed for REV creation and approval process will process in parallel. | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired |
|  | User tries to enter an incorrect ME code | | Appropriate error message will be displayed to the user that no such record was found |
|  | User tries to enter incorrect ME Name | | Appropriate error message will be displayed to the user that no such record was found |

### Use Case: UC-Institution ME Approval-007

Untitled Diagram (8)

|  |  |  |  |
| --- | --- | --- | --- |
| UC-007: Institution ME Approval | | | |
| **Description** | | This use case describes the Institution Merchant approval flow by the WL team | |
| **Actors** | | Insight Global, FSD Team | |
| **Pre-Condition** | | 1. New ME profile uploaded and submitted successfully 2. NMAS /MATCH /Risk Approval/Documentation/Post-Facto TRACE Approval (if any) done successfully | |
| **Post-Condition** | | 1. Institution ME profile(s) is approved successfully 2. Log file is created on successful approval | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | WL user will be logging into the Insight using his username and password | | The System captures the entered user credentials and validates the same from the backend. |
|  | WL user will select the Institution Merchant Approval link from the Insight screen | | The “Institution Merchant Approval” screen is displayed on the Insight screen |
|  | WL user will enter Merchant Code and search the record to approve | | The Insight screen should display all the records whose Institution ME Approval is pending |
|  | WL user will select the ME record and click on the Approve button | | The Insight screen will ask confirmation and on confirming, display the message “Request processed successfully” |
|  |  | | A log file is created after the request is processed. The Log file will contain brief details about merchant and status of the merchant – successful/unsuccessful |
| **Business Rules** | | | |
|  | For Institution Merchant approval, the new ME profile should be created and NMAS /MATCH /Risk Approval/Documentation/Post Facto trace Approval (if any) should be done successfully. | | |
|  | Institution ME approval will be done for all merchants (including Group ME). | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired |
|  | User tries to enter an incorrect ME code | | Appropriate error message will be displayed to the user that no such record was found |
|  | User tries to enter incorrect ME Name | | Appropriate error message will be displayed to the user that no such record was found |

### Use Case: UC-Generation of REV, POSF & MCOM file-008

REV file Generation (1)

|  |  |  |  |
| --- | --- | --- | --- |
| UC-008: Generation of REV, POSF & MCOM file | | | |
| **Description** | | This use case describes the generation of REV, POSF, MCOM file in the Rev Module | |
| **Actors** | | Rev Module, REV Team | |
| **Pre-Condition** | | 1. Institution Merchant Approval done successfully 2. New ME profile uploaded and approved in Insight | |
| **Post-Condition** | | 1. Terminal parameter file (REV) is created which is uploaded onto the terminal 2. POSF and MCOM file is created which is uploaded in the WL switch | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | REV team will be logging into the internal REV application of WL using his username and password | | The Rev module captures the entered user credentials and validates the same from the backend. |
|  | REV team will follow the below steps:   1. Click on REV Automation🡪New REV Creation 2. Select the Bank name from drop down list and click on Create REV 3. Click on View to check the list of REVs pending for generation 4. Select the records and click on create REV | | * Screen will display the record pending for REV Creation * The Rev file is uploaded onto the Terminal * After process, screen will say no records to be processed |
|  |  | | REV is generated successfully for the merchant in Insight database. |
|  |  | | * The System will generate the POSF and MCOM files from the rev module * The POSF and MCOM files will be uploaded in the WL Switch |
| **Business Rules** | | | |
|  | Verify REV file using standard document. | | |
|  | Terminal parameter file (REV) shall be created as per standard EMV format. The REV shall contain the following Mandatory and Optional Parameters:   |  | | --- | | **Mandatory Parameters** | |          Card Ranges | |          EMV Length | |          MID, TID | |          Connectivity (Telephone No etc.) | | **Additional Parameters ( Enable / Disable):** | |          Key Entry | |          Offline | |          Refund | |          Pre- Authorisation | |          Last 4 Digits | |          Force Settlement/Auto Settlement | |          Cash@POS – Txn Type | |          TIP Adjustment-Txn Type | | | |
|  | POSF and MCOM file shall be created as per the formats. | | |
|  | Once REV is generated for that merchant, FSD team will have to do installation Commissioning for which he need assets. | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | User enters incorrect Username & Password combination | | Appropriate error message will be displayed to user stating that the entered credentials are not incorrect. |

### Use Case: UC-Installation Request Commissioning-009

FSD Team (1)

|  |  |  |  |
| --- | --- | --- | --- |
| UC-009: Installation request commissioning | | | |
| **Description** | | This use case describes the asset creation, installation and REV deployment activities by the FSD Team | |
| **Actors** | | Insight, FSD Team | |
| **Pre-Condition** | | 1. Merchant created successfully in Insight 2. REV generated successfully | |
| **Post-Condition** | | 1. FSD team performs the asset creation of merchant 2. FSD team performs the installation and commissioning activities | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | FSD team will be logging into the Insight Global module using his username and password | | The Insight Global module captures the entered user credentials and validates the same from the backend. |
|  | **Asset Creation:**   1. Click on Masters🡪Asset🡪Add Asset 2. Create various Assets - Battery,Power Pack,Terminal and SIM (optional - only for GPRS terminal) 3. Enter all the asset details and click on the ‘Add’ button | | Screen should display the message ‘Asset added successfully’ |
|  | **Installation Commissioning:**  FSD team will select the Asset management link and follow the below steps:   1. Click on the Installation Request 2. Enter ME Code and search record.(user can also enter any of the search criteria) 3. Click on Request number link displayed in record 4. Enter the asset details and all mandatory details on commissioning page. 5. For selecting Asset ID click on Show button 6. Click on Search button to search asset details. 7. Select other asset like Battery, Power Pack and Terminal. 8. Click on Asset Code link to set it. 9. It will show all selected applications during created merchant. 10. Click on save button to complete the commissioning. | | Screen should display New Installation(Installation id) added successfully |
| **Business Rules** | | | |
| 1 | REV File is generated from the Rev module after which commissioning is performed | | |
| 2 | Asset details to be entered properly | | |
| 3 | Force (named as Auto in Insight Applicaton) settlement should be default enable excluding Hotels, Restaurants, Airline Ticket Booking Agents. | | |
| 4 | Last 4 digit and Refund should be default disabled. | | |
| 5 | Authorisation should be default enabled for All Merchants, all terminals. | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | User enters incorrect Username & Password combination | | Appropriate error message will be displayed to user stating that the entered credentials are not incorrect. |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired |
|  | User tries to enter an incorrect ME code | | Appropriate error message will be displayed to the user that no such record was found |
|  | User tries to enter incorrect ME Name | | Appropriate error message will be displayed to the user that no such record was found |

### Use Case: UC-Merchant Profile Change Request-010

MCR (1)

|  |  |  |  |
| --- | --- | --- | --- |
| UC-010: MCR Request | | | |
| **Description** | | This use case describes the MCR request raised and commissioned | |
| **Actors** | | Bank, Insight | |
| **Pre-Condition** | | Merchant is already created in Insight | |
| **Post-Condition** | | FSD performs the MCR commissioning activities | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | Bank user will be logging into the Insight module using his username and password | | The Insight module captures the entered user credentials and validates the same from the backend. |
|  | Bank user will follow the below steps to raise MCR request:   1. Select the option ME Profile Created🡪Merchant Profile Change Request🡪Add ME Profile Change request 2. Enter the ME code and search the record 3. Select the record and do the necessary changes and click on Submit | | Screen will display ME Profile updated successfully and Change Request (MCR ID) for Insight ME Added successfully |
| **Alternate Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | **MCR Bulk Upload:**  Bank user will follow the below steps to bulk upload MCR file:   * Click on ME profile Created🡪MCR upload * Browse the required file and click on Upload | | Success message should be displayed as File uploaded Successfully  Log file is generated after successful upload |
| **Business Rules** | | | |
|  | User will be able to change the ME parameters by inputting the details through fields provided -   * Request Date * Merchant Details * Branch Details * Merchant Address * MCC and TCC code * Mailing Address * Principle Owner Address * Other Merchant Details * Merchant MSF Details * Merchant Category / Rates & Fees * Document Checklist * RM Details | | |
|  | User can also perform the documentation checklist updation in the MCR request | | |
|  | User should upload the bulk MCR file in proper format | | |
|  | Bank can update the following fields under MCR Request. | | |
|  | CRN and \*Merchant account number change request to be handled under MCR change request workflow. | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | User enters incorrect Username & Password combination | | Appropriate error message will be displayed to user stating that the entered credentials are not incorrect. |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired |

### Use Case: UC-MCR Approval & Commissioning-011

MCR approval

|  |  |  |  |
| --- | --- | --- | --- |
| UC-011: MCR Approval & commissioning | | | |
| **Description** | | This use case describes the MCR request raised and commissioned | |
| **Actors** | | Bank, Insight | |
| **Pre-Condition** | | 1. Merchant already created in Insight 2. MCR request is raised | |
| **Post-Condition** | | Bank user performs the MCR commissioning activities | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | Bank user will be logging into the Insight module using his username and password | | The Insight module captures the entered user credentials and validates the same from the backend. |
|  | **MCR Approval:**  Bank user will follow the below steps to approve MCR request:   1. Go to Approval🡪Change Request Approval 2. Enter the ME code and click on Search 3. Select the record and enter Remarks and click Submit 4. Verify the log file generated | | * Screen will ask confirmation and on confirming will display a message stating “Request submitted successfully. Please check Log for Status and display log file” * Log file is generated after successful MCR approval |
|  |  | | MCR record changes will be reflected in the Insight and Kalkulus database. |
| **Alternate Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | **MCR Bulk Approval:**  Bank user will follow the below steps to approve bulk upload MCR file:   1. Select the Masters->Bulk Merchant Approval link 2. Enter the details and click on Search button 3. Select the record and click on the approve button to approve that MCR request for ME | | The Bulk Merchant Approval screen will display the particular record pending for approval |
| **Business Rules** | | | |
|  | Log file is generated after the MCR approval. The log file will contain the status of the MCR request whether approved or rejected along with the reason in case of rejection. | | |
|  | CRN and \*Merchant account number change request to be handled under MCR change request workflow. | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Bank user enters incorrect Username & Password combination | | Appropriate error message will be displayed to user stating that the entered credentials are not incorrect. |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired |

### Use Case: UC-Parameter Change Request & Commissioning-012

PCR

|  |  |  |  |
| --- | --- | --- | --- |
| UC-012: Parameter Change request & commissioning | | | |
| **Description** | | This use case describes the asset management activities by the FSD Team | |
| **Actors** | | Bank, Insight, Rev Module, FSD Team, REV Team | |
| **Pre-Condition** | | Pre generated TID/MID should be created  Commissioning done for the merchant successfully | |
| **Post-Condition** | | 1. FSD performs the Parameter change request commissioning 2. Terminal parameter file (REV) is created which is uploaded onto the terminal 3. POSF and MCOM file is created which is uploaded in the switch | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
| 1 | **Add new Parameter Change Request:**  Bank user will be logging into the Insight module using his username and password | | The Insight module captures the entered user credentials and validates the same from the backend. |
| 2 | Bank user will select the Parameter Change request link and follow the below steps:   1. Click on Add Parameter Change Request link. 2. Enter TID and search details. 3. Edit details and send request. | | * The Insight screen will display the existing Merchant, Terminal and Application Details * The Insight screen displays parameter Change Request(PCR ID) added successfully-MID |
|  |  | | REV file is generated (Refer [Use Case 008](#_Use_Case:_UC-Generation) for the same) |
| 4 | **PCR Commissioning:**  FSD team will login into the Insight Global module using his username and password | | The Insight Global module captures the entered user credentials and validates the same from the backend. |
| 5 | FSD team will select the Asset Management link and follow the below steps:   1. Click on Parameter Change Request link 2. Enter Assigned ME Code and search details 3. Click on Request Number link 4. Enter all the mandatory details and save it to commissioning the request | | System shows the request is commissioned |
|  |  | | System will generate the Rev file which is uploaded onto the Terminal |
|  |  | | System will generate the POSF and MCOM file which is uploaded in the switch |
| **Business Rules** | | | |
| 1 | Valid TID should be entered for Parameter change request | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | User enters incorrect Username & Password combination | | Appropriate error message will be displayed to user stating that the entered credentials are not incorrect. |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired |

### Use Case: UC-Application Activation Request & Commissioning-013

PCR (1)

|  |  |  |  |
| --- | --- | --- | --- |
| UC-013: Application Activation request commissioning | | | |
| **Description** | | This use case describes the asset management activities by the FSD Team | |
| **Actors** | | Bank, Insight, Rev Module, FSD Team, REV Team | |
| **Pre-Condition** | | Pre generated TID/MID should be created | |
| **Post-Condition** | | 1. FSD performs the Application activation request commissioning 2. Terminal parameter file (REV) is created which is uploaded onto the terminal | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
| 1 | **Raise Application Activation Request:**  Bank user will be logging into the Insight module using his username and password | | The Insight module captures the entered user credentials and validates the same from the backend. |
| 2 | Bank user will select the Asset Management option and follow the below steps:   1. Click on Application Activation Request link. 2. Click on Add Application Activation Request. 3. Enter TID and Search details 4. Select the application to activate from list and Send Request. | | * The screen displays the message “Application Activation Request (request\_id) added successfully’’ * The system receives the request and is sent for commissioning the same. |
| 4 | **Application Activation Request Commissioning:**  FSD team will login into the Insight Global module using his username and password | | The Insight Global module captures the entered user credentials and validates the same from the backend. |
| 5 | FSD team will select the Asset Management link and follow the below steps:   * Click on Application Activation Request * Enter Assigned ME Code and search record * Click on Request Number link. * Enter all mandatory details and save request | | System shows the request is commissioned |
|  |  | | System will generate the Rev file (Refer [Use Case 008](#_Use_Case:_UC-Generation) for the same) |
| **Business Rules** | | | |
|  | Valid TID should be entered for application activation request | | |
|  | User can select the option for asset swapping in the application activation request | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired |

### Use Case: UC-Application Reactivation Request & Commissioning-014

App React (1)

|  |  |  |  |
| --- | --- | --- | --- |
| UC-014: Application Reactivation Request | | | |
| **Description** | | This use case describes the asset management activities by the FSD Team | |
| **Actors** | | Bank, Insight, Rev Module, FSD Team, REV Team | |
| **Pre-Condition** | | Pre generated TID/MID should be created | |
| **Post-Condition** | | 1. FSD performs the Application re-activation request commissioning 2. Terminal parameter file (REV) is created which is uploaded onto the terminal | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
| 1 | **Raise Application Re-activation Request:**  FSD team will be logging into the Insight module using his username and password | | The Insight module captures the entered user credentials and validates the same from the backend. |
| 2 | FSD team will select the Asset Management option and follow the below steps:   1. Click on Application Reactivation Request link. 2. Click on Add Application Reactivation Request. 3. Enter TID and Search details 4. Select the application to re-activate from list and Send Request. | | The system receives the request and is sent for commissioning the same. |
| 3 |  | | System will generate the Rev file which is uploaded onto the Terminal |
| 4 | **Application Re-activation Request Commissioning:**  User will login into the Insight Global module using his username and password | | The Insight Global module captures the entered user credentials and validates the same from the backend. |
| 5 | User will select the Asset Management link and follow the below steps:   * Click on Application Activation Request * Enter ME Code and search record * Click on Request Number link. * Enter all mandatory details and save request | | System shows the request is commissioned |
| **Business Rules** | | | |
| 1 | Valid TID should be entered for application re-activation request | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired |

### Use Case: UC-Application De-Activation Request-015

AD

|  |  |  |  |
| --- | --- | --- | --- |
| UC-015: Application De-Activation Request | | | |
| **Description** | | This use case describes the asset management activities by the FSD Team | |
| **Actors** | | Bank, Insight, Rev Module, FSD Team, REV Team | |
| **Pre-Condition** | | Pre generated TID/MID should be created | |
| **Post-Condition** | | 1. FSD performs the Application re-activation request commissioning 2. Terminal parameter file (REV) is created which is uploaded onto the terminal | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | **Raise Application De-activation Request:**  Bank user will be logging into the Insight module using his username and password | | The Insight module captures the entered user credentials and validates the same from the backend. |
|  | Bank user will select the Asset Management option and follow the below steps:   1. Click on Application De-Activation Request link. 2. Click on Add Application De-Activation Request. 3. Enter TID and Search details 4. Select the application(s) to de-activate from list and Send Request. 5. Deactivate the required Application by selecting the date of deactivation besides the Application and click Send request | | The system receives the request and is sent for commissioning the same. |
|  | **Application De-activation Request Commissioning:**  FSD team will login into the Insight Global module using his username and password | | The Insight Global module captures the entered user credentials and validates the same from the backend. |
|  | FSD team will select the Asset Management link and follow the below steps:   * Click on Application De-Activation Request * Enter ME Code and search record * Click on Request Number link. * Enter all mandatory details and save request | | System shows the request is commissioned |
| **Business Rules** | | | |
| 1 | Valid TID should be entered for application de-activation request | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired |

### Use Case: UC-Asset Swapping Request-016

AS

|  |  |  |  |
| --- | --- | --- | --- |
| UC-016: Asset Swapping Request | | | |
| **Description** | | This use case describes the asset management activities by the FSD Team | |
| **Actors** | | Bank, Insight, Rev Module, FSD Team, REV Team | |
| **Pre-Condition** | | Terminal already installed | |
| **Post-Condition** | | Asset Swapping request is processed successfully | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
| 1 | Bank user will be logging into the Insight Global module using his username and password | | The Insight Global module captures the entered user credentials and validates the same from the backend. |
| 2 | **Raise Asset Swapping Request:**  Bank user will select the Asset management link and follow the below steps:   1. Click on Asset Management🡪Asset Swapping Request🡪Add Asset Swapping Request 2. Enter the TID and Click on Search 3. Select the required Asset model 4. Enter all the required details and click Send Request | | 1. Screen will display the message “Swapping Request (Req ID) added successfully” 2. The changes are updated in the Insight database |
|  | **Rev File Generation:**  FSD team will login to the Rev module with user credentials and follow the below steps:   1. Click on Rev Automation->Asset Swapping | | Rev file is generated |
| 4 | **Asset Swapping Request Commissioning:**  FSD team will select the Asset management link and follow the below steps:   1. Click on Asset Swapping Request 2. Enter ME Code and Click on Search 3. Select the record 4. Enter the Asset details and all other required details and click on Submit | | Screen will say Asset Swapping Commissioning completed successfully |
| **Business Rules** | | | |
| 1 | A valid TID should be entered for asset swapping request, otherwise the system will not take the TID | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired |

### Use Case: UC-Deinstallation Request-017

VIACQ (7)

|  |  |  |  |
| --- | --- | --- | --- |
| UC-017: Deinstallation Request | | | |
| **Description** | | This use case describes the deinstallation activities by the FSD team | |
| **Actors** | | Bank, Insight, FSD Team, REV Team | |
| **Pre-Condition** | | Terminal Already Installed | |
| **Post-Condition** | | The terminal is de-installed | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
| 1 | **Deinstallation Request:**  Bank user will be logging into the Insight module using his username and password | | The Insight Global module captures the entered user credentials and validates the same from the backend. |
| 2 | Bank user will select the Asset management link and follow the below steps:   1. Click Add Deinstallation Request 2. Enter the TID of the required Terminal and click search 3. Enter all the required details and click Submit | | Screen will display the message “Asset Deinstallation Request(Req ID) added successfully” |
| 4 | **Deinstallation Request Commissioning:**  FSD team will select the Asset management link and follow the below steps:   1. Click on De-installation Request 2. Enter ME Code and Click on Search 3. Select the record 4. Enter the details and click on Submit | | Screen displays Deinstallation Completed Successfully |
| **Business Rules** | | | |
| 1 | There is no REV file generation for Asset De-installation | | |
| 2 | A valid TID should be entered for asset deinstallation request, otherwise the system will not take the TID | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Timeout between the Insight portal and the server | | Appropriate error message will be displayed to the user stating the Session has been expired |



## Merchant Payment System (Kalkulus)

Merchant payments will contain all transaction settled by the merchant before cut-off time. MSF and Service Tax will be deducted from the sale amount. In addition to that, there may be debit/credit adjustments or refunds processed in the merchant payments. The net amount arrived will be paid to the merchants.

**Following are the steps involved in the same:**

* Merchant will have account with the specific Bank and the total payments (VISA, MasterCard and RuPay) shall be credited to this account on daily basis, else NEFT may be used as mode of payment credit to Merchant Account with other Bank. Bank to confirm on the same.
* BANK will have settlement accounts with Visa, MasterCard as well as NPCI.
* Merchant payment advises will be generated on daily basis.
* The merchant payment upload files need to be generated based on the Bank account numbers to which the MIDs of the merchant is mapped at the time of onboarding.
* There will be surcharge applicable on petrol/railway transactions.
* Surcharge for Maestro is applicable as per existing process i.e. as an acquirer WL India to present surcharge in the Outgoing file along with the transaction amount. Surcharge is not deducted at the time of Base I authorisation.
* Service tax and cess calculation - Service Tax and cess should be deducted for calculating Net Merchant Proceeds. X% Service Tax plus X% Swatch Bharat Cess and Kisan Kalyan Cess as Applicable (as applicable). The same is updated as per ongoing changes specified by Finance ministry to be incorporated from time to time post approval from Bank.
* Mode of Payment : Account Credit, NEFT
* Merchant payment will be done by Bank based on the Payment Upload file (TTUM).
* Separate chargeback recovery module shall be built in Phase II

kalkulus

Fig. Merchant Payment System

### ACCOUNTING / Fund flow for Merchant Payments

Bank needs to provide the following account details for Merchant Settlement:

* Visa Settlement Account
* MasterCard Settlement Account
* Maestro Settlement Account
* RuPay Settlement Account
* NEFT GL Account
* MSF (commission) account
* Service tax account
* Holdover/Release account
* Cash@POS Interchange Account
* Cash@POS Incentive Account

The Merchant Payment Accounting entry shall be passed by the WL Merchant Payment system through the below given entry:

|  |  |
| --- | --- |
| **DEBIT** | **CREDIT** |
| Debit VA Settlement A/c  Debit MC Settlement A/c  Debit RU Settlement A/c | Credit MSF A/c  Credit ST A/c  Credit ME A/c |

**Given Below is an example of fund flow of a merchant settlement transaction for Illustrative Purpose, however the actuals may differ.**

**Merchants having Bank’s current accounts:**

MasterCard INR 2000 and MSF is 200, SER.TAX  30          MERCHANT  A

Visa INR 3000 and MSF is 300,           SER.TAX  45

MasterCard INR 1000 and MSF is 100, SER.TAX  15          MERCHANT  B

Visa INR 4000 and MSF is 400            SER.TAX  60

**NEFT merchants**

MasterCard INR 500 and MSF is 50, SER.TAX  07.5       MERCHANT  C

Visa INR 300 and MSF is 30,              SER.TAX  04.5

MasterCard INR 600 and MSF is 60,  SER.TAX  09         MERCHANT  D

Visa INR 400 and MSF is 40               SER.TAX  06

Note: The Service Tax Rate has been considered @15% as per current Govt Regulations. However, this shall be updated as per revision in Govt Guidelines.

**In case of Normal Payment (This is the accounting entries that is passed by the WL Merchant Payment System that shall be available in the Merchant payment upload file i.e TTUM to be uploaded in BANK Banking system)**

|  |  |  |
| --- | --- | --- |
| **Account** | **DR/CR in INR** | **Remarks** |
| MasterCard settlement a/c | Dr 4100 | MerchantPayout/DDMMYY/’’No of Merchant count” |
| Visa settlement a/c | Dr 7700 | MerchantPayout/DDMMYY/’’No of Merchant count” |
| M/E   A/C (Merchant A) | Cr 4425 | BankPayout/DDMMYY |
| M/E   A/C (Merchant B) | Cr 4425 | BankPayout/DDMMYY |
| NEFT G/L (Merchant C/D) | Cr 1593 | BankPayout/DDMMYY (Should be Merchant wise) |
| MSF a/c | Cr 1180 | MSF payment for dd/mm/yyyy |
| SERVICE TAX | CR 127 | SER. TAX payment for dd/mm/yyyy |

**In case of hold release**

**First day(hold)**

|  |  |  |
| --- | --- | --- |
| **Account** | **DR/CR in INR** | **Narration** |
| MasterCard settlement a/c | Dr 4100 | Payment Hold for dd/mm/yyyy |
| Visa settlement a/c | Dr 7700 | Payment Hold for dd/mm/yyyy |
| Holdover a/c | Cr 4425 | Payment hold/MIDA/DDMMYY\* |
| Holdover a/c | Cr 4425 | Payment hold/MIDB/DDMMYY |
| Holdover a/c | Cr 705 | Payment hold/MIDC/DDMMYY |
| Holdover a/c | Cr 885 | Payment hold/MIDD/DDMMYY |
| MSF a/c | Cr 1180 | MSF payment for dd/mm/yyyy |
| SERVICE TAX | CR 127 | SER TAX payment for dd/mm/yyyy |

\*The Payment Hold entry shall be Merchant Wise or Transaction wise Credit into Holdover GL Account, as the case May be. There shall never be a consolidated entry into Bank Holdover GL Account.

**Release TTUM (Tickle Feed) entry will be**

|  |  |  |
| --- | --- | --- |
| **Account** | **DR/CR in INR** | **Narration** |
| Holdover a/c | Dr 4425 | Payment Release/MID A/DDMMYY |
| Holdover a/c | Dr 4425 | Payment Release/MID B/DDMMYY |
| ME A/c (Merchant A) | CR. 4425 | BankPayout/DDMMYY |
| ME A/c (Merchant B) | CR. 4425 | BankPayout/DDMMYY |
| Holdover a/c | Dr 705 | Payment Release/MID C/DDMMYY |
| Holdover a/c | Dr 885 | Payment Release/MID D/DDMMYY |
| NEFT G/L | Cr 1593 | Payment Release/MID D/DDMMYY (Should be Merchant wise) |

All Merchant Payment after Hold Release shall be Merchant Wise and Transaction Wise as the case may be.

**IN CASE OF REFUND TRANSACTION.**

|  |  |
| --- | --- |
| **DEBIT** | **CREDIT** |
| Debit Merchant A/c\* | Credit VA Settlement A/c\*  Credit MC Settlement A/c\*  Credit RU Settlement A/c\* |

\*The Narration shall be as per Bank Guidelines. : Merchant Refund/MIDA/DDMMYY

The payment will be uploaded in the Bank Banking system by the given TTUM file format attached as Annexure F.

### Use Case: UC-Batch Processing & EOD Processing-001

Batch Processing (1)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Use Case 001: Batch Processing & EOD Processing | | | | |
| **Description** | | This use case describes the batch processing and EOD processing that happens in the Kalkulus module | | |
| **Actors** | | Magnus, Kalkulus, REV Module | | |
| **Pre-Condition** | | 1. MCOM and POSF file should be already uploaded in the Switch 2. Settled Transaction Batches is obtained from the switch 3. Batch file is present for the Bank 4. CTL files are present for the Bank 5. Kalkulus login is available | | |
| **Post-Condition** | | Processed batches from the Kalkulus module to be uploaded in the Cronus | | |
| **Main Flow** | | | | |
| **Step** | **User Action** | | **System Action** | |
|  | WL user opens the form Kalkulus module and enters his username and password and clicks on Login | | The system captures the entered user credentials and validates the same.  The user is successfully logged into Kalkulus | |
|  | **ISO Batch Processing:**  To process the batches, user selects:   1. CPU Activities🡪EOD Process🡪EOD Kalkulus 2. WL user is displayed with a screen showing two options:  * **Multi EOD**: Process runs multiple times * **Final EOD**: Process runs only once  1. WL user selects one of the above options and clicks on “Continue” | | * Blank EOD is successfully executed * ISO batch file is processed successfully in the system and the system displays a message “Kalkulus processing is completed” | |
|  | WL user checks whether the data is properly inserted into the database-table when EOD is run. | | The RAW\_BTH table will contain data as per the ISO batch file uploaded | |
|  | WL user checks whether the successfully processed data is properly inserted into the database-table Valid\_BTH when EOD is run | | The Valid\_Bth table is verified in kalkulus schema | |
|  | WL user checks whether any error record data is inserted into the database-table Error\_bth when EOD is run | | The Error\_Bth table is verified in kalkulus schema | |
|  |  | | **History Movement:**  The data processed are automatically archived into the database table as part of the history movement process | |
|  | **EOD Report Generation:**   1. After successful batch file processing, EOD Reports are generated on server 2. WL user can check the reports on the server location. 3. WL user can performs the following steps in the Kalkulus module to generate reports: 4. Click on CPU Activiies -> Reports-> Daily All bank’s reports 5. Select a report and enter the required details 6. Click on Execute 7. Download the report from the server | | * EOD Reports are generated on server location * Following reports are generated after Batch File Processing:   1.BA25081  2.DIF000552508  3.DLRC-00055-260816  4.Prolog-260816-153133  5.RECON-260816  6.SURCHARGE-00055-260816   * Processed Batch Report: It will contain all the successfully processed transactions * DIF Report: It will contain all the Petro merchant transactions along with the surcharge details * DLRC Report: It will contain all the Daily Reconciliation Reports and details about all scheme wise transactions * Prolog Report: It will contain all the EOD processing details * Recon Report: It will contain all the Recon transaction details according to Bank code * Surcharge Report: It will contain all the Surcharge details of Petro merchant transactions for various card numbers | |
| **Business Rules** | | | | |
|  | Settled transaction batches from the Switch are uploaded into the Kalkulus.  The batch obtained from the switch is a bankwise raw batch which is the input file to the Kalkulus system | | | |
|  | **Data Processing in Kalkulus:**   1. Data Loading: Data is extracted from the batch and inserted in the database table 2. Validation: The field data (which is extracted from the batch) will be checked with the data present in the Kalkulus database 3. Successful data from validation i.e. batches are stored in separate table(Valid\_BTH) and the rejected data is discarded in other table(Error\_BTH) 4. Processing starts on valid batches. Calculations are done for the following and the data is stored in a table:  * TXN Amount * MSF * Commission * Service Tax * Surcharge | | | |
|  | If TIP transactions are present in the batch, the batch is processed successfully | | | |
|  | If Sale/Purchase transactions are present in the batch, batch is processed successfully | | | |
|  | Pre auth and completion transactions in batch are processed successfully | | | |
|  | Cash at POS transactions in batch are processed successfully | | | |
|  | Key entry transactions in the batch are processed successfully | | | |
|  | Offline transactions in batch are processed successfully | | | |
|  | Processed batch will contain the Surcharge amount along with the transaction amount | | | |
| **Exceptional Flow** | | | | |
| **Sr. No.** | **Exception** | | | **Error Message/Action** |
|  | Batch file contains spaces in RRN field | | | Batch is processed successfully and present in valid\_bth |
|  | Duplicate batch file is taken | | | Batch is not processed and is present in error\_bth |
|  | Invalid processing code in batch | | | Batch is processed successfully and present in valid\_bth |
|  | Invalid POS Entry mode in batch | | | Batch is processed successfully and present in valid\_bth |
|  | Refund transaction present in batch | | | Batch is processed successfully and present in valid\_bth |
|  | DCC transactions in batch | | | Batch is not processed and is present in error\_bth |
|  | Invalid merchant is present in batch | | | Batch is not processed and is present in error\_bth |
|  | Header/trailer missing in batch | | | Batch is not processed and is present in error\_bth |
|  | Different acq bin is present in batch | | | Batch is processed successfully and present in valid\_bth |
|  | International transactions is present in batch | | | Batch is processed successfully and present in valid\_bth |
|  | Junk characters are present in card no. transactions in batch | | | Batch is not processed and is present in error\_bth |
|  | Batch total has mismatch | | | Batch is not processed and is present in error\_bth |
|  | Non numeral currency code is present in acquirer currency code field in batch | | | Batch is not processed and is present in error\_bth |
|  | User enters incorrect Username & Password combination | | | Appropriate error message will be displayed to user stating that the entered credentials are not incorrect. |
|  | User doesn’t enters username or password and clicks on the Submit button | | | Appropriate message will be displayed to user stating that the required fields are mandatory |

### Use Case: UC-Report Generation from Kalkulus-002

VIACQ (6)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Use Case 002: Report Generation from Kalkulus | | | | |
| **Description** | | This use case describes the CPU daily report generation from the Kalkulus module | | |
| **Actors** | | Magnus, Kalkulus | | |
| **Pre-Condition** | | Batch file is run successfully | | |
| **Post-Condition** | | CPU daily reports is generated and is downloaded from the server | | |
| **Main Flow** | | | | |
| **Step** | **User Action** | | **System Action** | |
|  | WL user opens the form Kalkulus module and enters his username and password and clicks on Login | | The system captures the entered user credentials and validates the same.  The user is successfully logged into Kalkulus | |
|  | WL user verifies the following CPU Daily Reports is generated after Report generation is done:   1. Domestic-Debit\_txns 0055.TXT 2. ALLTXN-00055.TXT 3. BRN-00055.SUM 4. COMM-TAX-00055.TXT 5. MEDETAILS-00055.TXT 6. ME-VOL-00055.TXT 7. MSD-00055.TXT 8. NEFT-00055.TXT 9. PAY-00055.TXT 10. PAY-SUM-00055.TXT 11. RCT-00055.TXT 12. TTUM-00055.TXT 13. UPD-00055.SUM 14. FIR-00055.TXT 15. FIR-00055.SUM   User can check the CPU Daily Report on the server location | | * The mentioned reports are generated after CPU Daily Report generation * CPU Daily Report are generated on the server location | |
|  | WL user performs the following steps to generate the FIRC report:   1. Click on CPU Activities->Reports->Daily All banks Report->Daily FIRC Report 2. Select Bank code-name from drop down menu 3. Click on Execute->Execute   User downloads the report from the server | | * The screen displays the message   'FIRC Report generated on server'   * The FIR-00055.SUM and FIR-00055.TXT reports will be generated on server location | |
| **Business Rules** | | | | |
|  | The Domestic-Debit\_txns 0055.TXT report will contain all the Domestic Debit transactions details alongwith MSF details  The COMM-TAX-00055.TXT report will contain all the transaction details along with their Commission and Service tax details  The MEDETAILS-00055.TXT report will contain all the merchants details and their transactions details alongwith MSF details  The ME-VOL-00055.TXT report will contain all merchants transaction details summary  The MSD-00055.TXT report will contain all merchants payment-settlement details  The NEFT-00055.TXT report will contain NEFT merchant’s payment details  The PAY-SUM-00055.TXT report will contain merchants' payment summary details  The RCT-00055.TXT report will contain all the Rupay Card Transaction details  The TTUM will contain all the payment details along with the individual payment entries for different accounts  The UPD-00055.SUM will contain the Payment Summary to different schemes and account alongwith MSF details  The FIR-00055.TXT will contain all the International Card Transaction details along with the configured USD rate and converted amounts  The FIR-00055.SUM report will contain the summary of the International Card Transaction details along with the configured USD rate and converted amount | | | |
| **Exceptional Flow** | | | | |
| **Sr. No.** | **Exception** | | | **Error Message** |
|  | User enters incorrect Username & Password combination | | | Appropriate error message will be displayed to user stating that the entered credentials are not incorrect. |
|  | User doesn’t enters username or password and clicks on the Submit button | | | Appropriate message will be displayed to user stating that the required fields are mandatory |

### Use Case: UC-Merchant Payment Advice report generation-003

VIACQ (5)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Use Case 003: Merchant Payment Advice report generation | | | | | |
| **Description** | | | This use case describes the merchant payment advice report generation | | |
| **Actors** | | | Magnus, Kalkulus | | |
| **Pre-Condition** | | | 1. Batch File run Successfully 2. New executables copied | | |
| **Post-Condition** | | | 1. MPC report is generated from the Kalkulus module 2. Email is sent to the Merchant about merchant payment advice report | | |
| **Main Flow** | | | | | |
| **Step** | **User Action** | | | **System Action** | |
| 1 | WL user opens the form Kalkulus module and enters his username and password and clicks on Login | | | The system captures the entered user credentials and validates the same.  The user is successfully logged in Kalkulus | |
| 5 | WL user performs the following steps to generate the merchant payment advice:   1. Click on CPU Activities🡪Reports🡪Daily All banks Report🡪MPC Report-Non DCC 2. Select Bank code-name from drop down menu 3. Click on Execute | | | * Report is generated on local machine * The screen will show a pop up window with a message which when selected as OK would display the path where the report is generated | |
|  | **Log File generation**:  User performs the following steps to check whether log file is generated after MPC report generation:   1. Click on CPU Activities🡪Reports🡪Daily All banks Report🡪MPC Report-Non DCC 2. Select Bank code-name from drop down menu 3. Click on Execute 4. On the log window, Click on Actions🡪Show Log | | | Log file will display the report generation date and time details | |
|  | **Email sent to the merchant:**   1. User opens the WL internal application, enters his username and password and clicks on Login 2. User selects the Institution and clicks on Generate | | | * The system captures the entered user credentials and validates the same. * Email will be sent to the respective Email ID. * Screen will display the message: ‘Email Statement Process has been done. Kindly Check log: *<<location of the log report>>’* | |
| **Business Rules** | | | | | |
|  | MPC Report generated for each merchant will contain all the transaction details along with the proper amounts | | | | |
|  | The Email Log Report will contain proper MID and the email Ids with status as 'Successfully sent' with Date and Time | | | | |
|  | In the case where the merchant’s email ID is not available in the database, the email will not be sent to that ME and the same error can be found in the Email log report | | | | |
| **Exceptional Flow** | | | | | |
| **Sr. No.** | | **Exception** | | | **Error Message** |
|  | | User enters incorrect Username & Password combination | | | Appropriate error message will be displayed to user stating that the entered credentials are not incorrect. |
|  | | User doesn’t enters username or password and clicks on the Submit button | | | Appropriate message will be displayed to user stating that the required fields are mandatory |

### Use Case: UC-TTUM File Generation-004

VIACQ (4)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Use Case 004: TTUM File Generation | | | | |
| **Description** | | This use case describes the TTUM file report generation | | |
| **Actors** | | WL user, Kalkulus | | |
| **Pre-Condition** | | 1. Batch File run Successfully 2. New executables copied | | |
| **Post-Condition** | | TTUM generated successfully and tallied | | |
| **Main Flow** | | | | |
| **Step** | **User Action** | | **System Action** | |
|  | WL user opens the form Kalkulus module and enters his username and password and clicks on Login | | The system captures the entered user credentials and validates the same.  The user is successfully logged in Kalkulus | |
|  | WL user performs the following steps to generate the TTUM report:   1. Select CPU Activities🡪Reports 2. Select All Bank reports 🡪CPU Daily report | | The TTUM report is generated on the server location: *<<server location path>>*  Refer [Annexure F](#_Annexure_1) for sample TTUM report. | |
| **Business Rules** | | | | |
|  | The TTUM should be tallied i.e. the Debit & Credit accounts are tallied. (Debit=Credit) | | | |
| **Exceptional Flow** | | | | |
| **Sr. No.** | **Exception** | | | **Error Message** |
|  | User enters incorrect Username & Password combination | | | Appropriate error message will be displayed to user stating that the entered credentials are not incorrect. |
|  | User doesn’t enters username or password and clicks on the Submit button | | | Appropriate message will be displayed to user stating that the required fields are mandatory |

### Use Case: UC-Hold and Release Functionality-005

VIACQ (2)

|  |  |  |  |
| --- | --- | --- | --- |
| Use Case 005: Hold and Release Functionality | | | |
| **Description** | | This use case describes the hold and release functionality of the payment transactions. | |
| **Actors** | | WL user, Kalkulus | |
| **Pre-Condition** | | Hold and release URL should be available | |
| **Post-Condition** | | 1. Transaction record will be held/released 2. Hold report and Release report can be generated | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | WL user opens the Hold and Release URL  WL user enters his username and password and clicks on Login | | The system captures the entered user credentials and validates the same. |
|  | WL user performs the following steps to check the hold functionality for the settled transactions:   1. Click on Payment Hold option 2. Select the bank code from the drop down menu 3. Enter required search criteria and click Execute | | The system screen will display all the transactions according to the search criteria |
|  | **Hold a transaction:**  WL user performs the following steps to hold a particular transaction/merchant payment:   1. Click on Payment Hold option 2. Select the bank code from the drop down menu 3. Enter required search criteria and click Execute 4. Select the record and click Hold | | The system screen will display 'record updated' message. |
|  | WL user performs the following steps to check the release functionality for the settled transactions:   1. Click on Payment Release option 2. Select the bank code from the drop down menu 3. Enter required search criteria and click Execute | | The system screen will display all the transactions that were held |
|  | **Release a transaction:**  WL user performs the following steps to release a particular transaction/merchant payment:   1. Click on Payment Release option 2. Select the bank code from the drop down menu 3. Enter required search criteria and click Execute 4. Select the record and click Release | | The system screen will display 'record updated' |
|  | **Hold Report Generation:**  WL user performs the following steps to generate a Hold report:   1. Click on Hold and Release report option 2. Select the Bank code-name 3. Select Report type as Hold 4. Enter the date and click Run | | Report will be generated on server location.  The system screen will display the message 'Report generation is completed'. Refer [Annexure E](#_Annexure_1) for sample payment Hold / Release reports |
|  | **Release report Generation:**  WL user performs the following steps to generate a Release report:   1. Click on Hold and Release report option 2. Select the Bank code-name 3. Select Report type as Release 4. Enter the date and click Run | | Report will be generated on server location.  The system screen will display the message 'Report generation is completed'. Refer [Annexure E](#_Annexure_1) for sample payment Hold / Release reports |
| **Business Rules** | | | |
|  | Any particular transaction that is held for payment can be released next day only | | |
|  | In case of Payment Holdover / Release, below mentioned entry is passed.  **For Hold:**   |  |  | | --- | --- | | **DEBIT** | **CREDIT** | | Debit VISA Settlement A/c  Debit MC Settlement A/c  Debit Rupay Settlement A/c | Credit MSF A/c  Credit ST A/c  Credit HoldOver A/c |   **For Release:**   |  |  | | --- | --- | | **DEBIT** | **CREDIT** | | Debit HoldOver A/c | Credit ME A/c  Credit NEFT GL A/c | | | |
|  | Based on the Bank’s business rules , WL will Hold/Release the payments | | |
|  | Customer will contacted through phone call or through email in any payment hold transaction. | | |
|  |  | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | User enters incorrect Username & Password combination | | Appropriate error message will be displayed to user stating that the entered credentials are not incorrect. |
|  | User doesn’t enters username or password and clicks on the Submit button | | Appropriate message will be displayed to user stating that the required fields are mandatory |

### Use Case: UC-VIACQ Module-006

VIACQ

|  |  |  |  |
| --- | --- | --- | --- |
| Use Case 006: VIACQ Module report generation | | | |
| **Description** | | This use case describes the report generation from the VIACQ module | |
| **Actors** | | Bank User, VIACQ module | |
| **Pre-Condition** | | VIACQ URL and credentials are available | |
| **Post-Condition** | | Various reports are generated and can be downloaded from the VIACQ screen | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | Bank user opens the VIACQ URL  Bank user enters his username and password and clicks on Login | | The system captures the entered user credentials and validates the same. |
|  | Bank user can view the following reports by clicking on the VIACQ link:   1. ME level report 2. ME Details 3. Card Search 4. Zone Level report 5. MCC level report 6. Commission report 7. Commission Adv report | |  |
|  | To download any of the above mentioned reports, Bank user will follow the below steps:   1. Click on the report to be downloaded 2. Enter the required search criteria 3. Click Search | | 1. System will prompt a message asking whether to download the file 2. The required report can be downloaded in the system |
| **Business Rules** | | | |
|  | ME Details report can only be viewed cannot be downloaded. | | |
|  | User licenses upto four users are given to the Bank out of which one or two can be Admin user and the rest is a normal user  The Admin user will be able to download the reports whereas a normal user can only view the reports | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | User enters incorrect Username & Password combination | | Appropriate error message will be displayed to user stating that the entered credentials are not incorrect. |
|  | User doesn’t enters username or password and clicks on the Submit button | | Appropriate message will be displayed to user stating that the required fields are mandatory |

* 1. Terminal

Terminal application will be fully EMV complaint.

Terminal application will have a feature of Force settlement (This is the feature wherein if a ME transacts on a particular day and does not settle the batch before midnight, post which if the ME tries to make a transaction the terminal prompts batch settlement. The terminal does not allow a transaction until and unless the previous days batch is settled) feature. This will apply on every merchant type except Hotel merchants.

The following types of transactions should be supported by this application:

|  |  |  |
| --- | --- | --- |
| **Transaction Types** | **Scheme Support** | **Online / Offline** |
| Sale | All Schemes | Online |
| Void | All Schemes | Online |
| Reversal | All Schemes | Online |
| Refund | VISA / MC | Offline |
| Pre-Auth | VISA / MC | Online |
| Pre-Auth completion | VISA / MC | Online |
| TIP Adjust | All | Offline |
| Cash Back Only | All | Online |
| Purchase with Cash Back | All | Online |
| Batch Settlement | All Schemes | Online |
| Batch Upload | All Schemes | Online |
| Settlement after Batch Upload | All Schemes | Online |
| VAS - balance enquiry | Only on Maestro Cards | Online |

**Note:** The refund transactions for RuPay require the Original RRN along with the Transaction as per guidelines by NPCI. The same shall not be supported through the Terminal and it shall be processed offline through the Bank’s User Access of RGCS Portal provided by NPCI.

Terminal

### Terminal Specifications:

|  |  |
| --- | --- |
| Communication Mode supported: | * PSTN * GPRS * Internet (WIFI) * CDMA * Broadband * VSAT |
| Types of card supported on Terminal | * Magstrip * Smart Card * NFC |
| POS device Capabilities: | * Display Amount * PIN Request * Insert /Swipe/ Tap Functionality * Mandate Insert if it is a Chip Card * Encrypt PIN and PAN Data with separate TLE and UKPT keys * Fall Back Mechanism as per EMV standards * Display final Status message * PIN verified, No Signature Required Implementation as per Scheme Recommendation * PAN should be by default masked for customer copy, merchant copy & settlement reports printed by the terminal. |

### KEY Management

* The POS terminal will use unique DUKPT TDES Encryption methodology to encrypt the PIN and crucial data.
* Master Clear component to be used for decrypting the IKEY need to be injected by the Terminal vendor in manufacturing process
* Keys will be shared with manufacturer by WL HSM as per the standard agreed during agreement process.
* The data which will be encrypted will be track2 or PAN number.

### Application Download

* The POS terminal is received by the FSD team with OS and Application Manager loaded in it.
* The Application is downloaded from TMS with the corresponding Input files.
* Input files like logo file, Input file containing details of NII, Merchant ID and terminal ID etc.
* Application, input file and Product File download can be initiated from terminal without user interference using RTM functionality.
* RTM will be supported by all terminal.
* Vendor should provide hot key to download the application and corresponding files directly from TMS.

**Note:** The application development of the terminal will be managed by the Bank’s vendor as per WL application requirements.

#### Use Case: UC-Initialization-001

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Use Case 001: Initialization | | | | |
| **Description** | | | This use case describes the initialization process in the terminal machine | |
| **Actors** | | | Terminal, Host | |
| **Pre-Condition** | | | The Rev file should be downloaded onto the terminal | |
| **Post-Condition** | | | Chargeslip is printed after successful transaction | |
| **Main Flow** | | | | |
| **Step** | | **User Action** | | **System Action** |
|  | | 1. User selects the Telium Manager option on the EDC machine 2. User will be able to view the various menu options under ‘Telium manager’ 3. To configure the basic terminal setup, user will go to the ‘Initialization’ option from the menu 4. Under Initialization option, user will be able to configure the following settings:  * Parameters: Includes parameters like date/time, language, terminal number, currency, pabx, pinpad, swipe, serial no, network access, cash connection, TMS * Hardware: Includes modem setup, energy save, display, proxy set * Password: Includes setting up a new password * Header * Beep on Key | | * Terminal will display the appropriate options on the menu screen as per the user’s selection * Terminal will save the information of the settings that were changed * Terminal will print the receipt/charge slip after successful changes applied |
|  | | **Evolution:**   1. User selects the Evolution option under Telium Manager on the EDC machine 2. User is prompted with two options:  * Load * Remote Load  1. User selects the Remote Load option 2. The system prompts the user to enter the Rev no. | | Terminal will remotely load the REV file from the TMS by connecting to the TMS through appropriate channels like IP/GPRS/ISDN/Modem |
| **Business Rules** | | | | |
|  | The Rev file can be loaded either via the process of initialization on the terminal through remote download or via LLT | | | |
|  | In the case when the Rev file is already present in the terminal, the initialization process would take the file from the terminal for loading irrespective of whether it is locally downloaded or not | | | |
|  | AGN file is loaded onto the terminal via LTT | | | |
|  | Telium Manager is used to configure OS related or system related settings | | | |
| **Exceptional Flow** | | | | |
| **Sr. No.** | **Exception** | | | **Error Message/Action** |
|  | Connection timeout between the terminal and host | | | Appropriate error message will be displayed to the user on the terminal screen |

#### Use Case: UC-Key Exchange Transaction-002

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Use Case 002: Key Exchange | | | | |
| **Description** | | This use case describes the key exchange process that happens in on the POS terminal | | |
| **Actors** | | Terminal, Host | | |
| **Pre-Condition** | | Rev file should be downloaded onto the terminal and terminal should be initialized | | |
| **Post-Condition** | | Chargeslip is printed after successful transaction | | |
| **Main Flow** | | | | |
| **Step** | **User Action** | | | **System Action** |
|  | **Terminal Input:**  User selects the specified key for Key Exchange Transaction | | | **Terminal Output:**   * Terminal will initiate the transaction * The terminal will dial the host. * Terminal will display the message ‘Key Exchange successful’. * It will store the working Key received from host and generate Pin block |
|  |  | | | **Host**:   * Host checks whether the terminal is sending the Key request packet as per the host message specifications (See [Appendix H](#_Annexure)) * Checks the Proc code * Checks the invoice no. shouldn’t get incremented |
| **Alternate Flow** | | | | |
| **Step** | **Scenario** | | **User/System Action** | |
|  | User presses the Cancel button while Key Exchange | | | Terminal will not take Cancel command and will process the transaction |
| **Business Rules** | | | | |
|  | In Key Exchange transaction, the corresponding key part should be present on Host otherwise it fails | | | |
| **Exceptional Flow** | | | | |
| **Sr. No.** | **Exception** | | | **Error Message** |
|  | Key Exchange Failure | | | Terminal will display the message ‘Key Exchange Failed’ and will not allow to do Pin based credit transaction. |

#### Use Case: UC-Online Sale-003

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Use Case 003: Online Sale | | | | |
| **Description** | | | This use case describes the online sale transaction that happens in the POS terminal | |
| **Actors** | | | Terminal, Host | |
| **Pre-Condition** | | | The Rev file should be downloaded onto the terminal and the parameters should be initialized | |
| **Post-Condition** | | | Chargeslip is printed after successful transaction | |
| **Main Flow** | | | | |
| **Step** | | **User Action** | | **System Action** |
|  | | **Card Swipe:**   1. User selects the Sale option on the EDC machine 2. User swipes the card 3. User enters the amount | | 1. Terminal will display the transaction name 2. Terminal will ask for swiping the card after selecting online Sale Option. 3. The terminal system will read the card details from magnetic strip. 4. Terminal will ask to Enter the amount 5. It will verify the card number in the card range, Expiry date and the Amount. It will dial the configured telephone number. 6. Terminal will display the Approval code after successful transactions 7. Terminal will print the receipt/charge slip after the transaction |
|  | | **Manual Entry:**   1. User selects the Sale option on the EDC machine 2. User enters the card number 3. User enters the expiry date 4. User enters the amount | | 1. Terminal will display the transaction name 2. Terminal will ask for entering the card number after selecting online Sale Option. 3. Terminal will verify the Luhn and the card number in Card Range 4. Terminal will ask to enter the Expiry date, Amount and verifies the same 5. After the amount is entered, terminal will dial to the host 6. Terminal will display the Approval code after successful transactions 7. Terminal will print the receipt/charge slip after the transaction |
|  | | **EMV:**   1. User selects the Sale option on the EDC machine 2. User inserts the card 3. User enters the amount | | 1. Terminal will display the transaction name 2. Terminal will ask to insert the card to the EDC machine after selecting online Sale Option. 3. The terminal will read the card details from chip; Verify the Luhn and the card number in Card Range 4. Terminal will ask to Enter the amount 5. After the amount is entered, terminal will dial to the host 6. Terminal will verify the expiry date and the amount 7. Terminal will display the Approval code after successful transactions 8. Terminal will print the receipt/charge slip after the transaction |
|  | |  | | **Host**:   1. Host checks whether the terminal is sending the online sale (swipe/manual/EMV) request packet as per the host message specifications (See [Appendix H](#_Annexure)) 2. Checks the Terminal totals should get updated by the transaction amount 3. Checks the Terminal is sending all the mandatory fields to the host 4. Checks for the Invoice no and Stan increment 5. Checks receipt contents: should print Merchant headers,Txn time, Txn date, MID, TID, Batch No, Invoice No,Txn Name,Card No, Card type, Exp Date, Card-holder’s Name, Amount, Auth Code, RRN, Disclaimer, Signature space and footer correctly.   **Note:**  In the case of Cash Advance:   1. The packet is the same as the online sale packet. 2. An appropriate disclaimer message is printed in the chargeslip for this transaction.   In the case of Sale with cashback or cashback:   1. User will be prompted for the options: 1) Sale 2) Sale with cashback 3) Cashback 2. In case Sale is selected, then normal sale transaction will be processed 3. In case Sale with Cash Back is selected, terminal to prompt for Sale amount and cash back amount separately. 4. A single chargeslip will be printed giving details of both sale & cash back and Total. (no adjustment sale is permitted). However Void of this transaction is allowed. No offline transaction is permitted. Transaction type will be printed as “Sale & Cash Back”. 5. In case Cash Back is selected, terminal to prompt for Cashback amount and the chargeslip to be printed as a Cash Back chargeslip. Transaction type to be printed as “Cash Back” For Cash Back transactions. 6. An appropriate disclaimer message is printed in the chargeslip for this transaction. |
| **Alternate Flow** | | | | |
| **Step** | **Scenario** | | | **User/System Action** |
|  | User tries to swipes the card which is not configured in the card range | | | Terminal will not proceed with the transaction and display appropriate error message to the user |
|  | User tries to enter the card number which is not configured in the card range | | | Terminal will not proceed with the transaction and display appropriate error message to the user |
|  | User enters a card number with invalid Luhn (Invalid Card) | | | Terminal will check the Luhn as per the defined logic. It will not proceed with the transaction and will display the message 'Luhn check Failed' |
|  | User swipes an expired card | | | Terminal will read the card details from mag stripe, verifies the card number and the expiry date.  Terminal will not proceed with the transaction and will display the message 'Expired Card' |
|  | User enters a card number entered with expiry date less than the current date | | | Terminal will verify the card number and the expiry date.  Terminal will not proceed with the transaction and will display the message 'Expired Card' |
|  | User enters a card number entered with expiry date in invalid format | | | Terminal will verify the card number and the expiry date.  Terminal will not proceed with the transaction and display message 'Expired Card' |
|  | User swipes a card swiped and enters an invalid amount | | | Terminal will read the card details from mag stripe and verify the following:   * Card number * Expiry date * Amount   Terminal will not proceed with the transaction and will display the message 'Invalid Amount' |
|  | User enters a card number entered with an invalid amount | | | Terminal will verify the following:   * Card number * Expiry date * Amount   Terminal will not proceed with the transaction and display message 'Invalid Amount' |
|  | User swipes a card and presses the cancel button | | | Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User swipes a card, enters the amount and presses the cancel button | | | Terminal will read the card details from mag stripe; verify the card number and expiry date.  Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User swipes the card, enters the amount and presses the cancel button before connecting to host | | | Terminal will read the card details from mag stripe; verify the card number and expiry date  Terminal will not proceed with the transaction and reset itself to idle mode. At host, the invoice no. will not be incremented |
|  | User swipes the card, enters the amount and presses the cancel button after receiving the approval code | | | Terminal will read the card details from mag stripe; verify the card number and expiry date  Terminal will not take the cancel command after receiving the approval code. It will proceed with the transaction  Host will check the following:   * Request packet * Terminal totals * Invoice no & Stan no. * Receipt contents |
|  | User enters the Card no., expiry date and then presses the cancel button | | | Terminal will not proceed with the transaction and reset itself to idle mode.  At host, the invoice no. will not be incremented |
|  | User swipes/inserts a damaged chip card and enters the amount | | | Appropriate error message to be displayed to the user. However, the user can manually enter the card details. |
|  | User inserts a card, enters the amount and press cancel button before connecting to host | | | Terminal will read the card details from the chip and verify the following:   * Card number * Expiry date * Amount   Terminal will not proceed with the transaction and reset itself to idle mode. Appropriate message will be displayed stating the transaction is declined. At host, the invoice no. will not be incremented. |
| **Business Rules** | | | | |
|  | Expiry Date on the card should not be less than the current date | | | |
|  | The Terminal totals should get updated by the transaction amount | | | |
|  | In case of online transaction – Manual/EMV, the terminal verifies the Luhn | | | |
|  | If a particular card is not configured in the card range then the terminal should not proceed with the transaction | | | |
|  | Sale with Cashback and Cashback feature is supported only for Indian Debit Cards. Cardholder can withdraw money at a merchant location. Cash withdrawal could accompany a purchase transaction also. | | | |
| **Exceptional Flow** | | | | |
| **Sr. No.** | **Exception** | | | **Error Message/Action** |
|  | Connection timeout between the terminal and host | | | Appropriate error message will be displayed to the user on the terminal screen |

#### Use Case: UC-Cash@POS-004

# CASH@POS TRANSACTIONS

The terminal shall process the Cash Back transactions under this transaction type.

Cashback amount shall be accepted in the Cash Back amount for both Cash Back and Purchase with Cash Back transactions, for which the Merchant shall provide equivalent Currency Notes.

* As per the new mandate of RBI for cash@ POS, the limit cash that can be retrieved by a customer/ cardholder at the POS terminal has been defined Location wise basis Tiering of the Cities.
* There is a limit that is applicable per cardholder for the amount that can be withdrawn by a customer/ cardholder against his debit/prepaid card per day.
* Cash@ POS entitlement is applicable for a debit/open loop prepaid cards only.
* The cash@ POS limit shall be enhanced based on the tier wise classification of the cities – the cities/centers shall be classified from Tier I to Tier IV.
* The cash@ POS limit for Tier I and Tier II centers shall be retained to 1000 INR; for Tier III to Tier IV, the limit shall be 2000 INR.

Attached is the RBI Circular for reference.



* The tier classification (tier I to VI) shall be mapped to branch code of the bank e.g. if bank’s branch code for branch located at Andheri (Mumbai) is 0041, the tier mapping shall be done as branch code 0041 to tier.

(in the above example, if tier is considered as T1, then mapping shall be as 0041 as T1, irrespective of the location of the branch).

* The branch master of the bank’s branch with the tier mapping of the regions shall be shared by the bank with WL, which shall be uploaded and maintained in WL system.

One time upload of branch code – tier mapping shall be done by WL.

Once the master has been uploaded, every time the branch master is updated by the bank/WL user (in the web module for branch master), the Tier of the branch code shall be updated.

|  |  |  |  |
| --- | --- | --- | --- |
| Use Case 004: Cash@ POS transactions | | | |
| **Description** | | This use case describes the cashback and purchase with cashback transactions that happens on the POS terminal | |
| **Actors** | | Terminal, Merchant | |
| **Pre-Condition** | | Rev file should be downloaded onto the terminal and the parameters are initialized | |
| **Post-Condition** | | Chargeslip is printed after successful transactions | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | **Cashback:**   1. User selects the Cashback option on the EDC machine 2. User swipes/manually enters the card details 3. User enters the amount and selects the Go button | | 1. The terminal system will read the card details from magnetic strip. 2. It will verify the card number in the card range, Expiry date, Amount. It will dial the configured telephone number. 3. Terminal will display the Approval code after successful transactions 4. Terminal will print the receipt/charge slip after the transaction |
|  | **Sale + Cashback:**   1. User selects the Sale with Cashback option on the EDC machine 2. User swipes/manually enters the card details 3. User enters the amount and selects the Go button 4. User then enters the cashback amount and selects the Go button | | 1. The terminal system will read the card details from magnetic strip. 2. It will verify the card number in the card range, Expiry date, Amount. It will dial the configured telephone number. 3. Terminal will display the Approval code after successful transactions 4. Terminal will print the receipt/charge slip after the transaction |
|  |  | | **Host:**   1. Host checks whether the terminal is sending the request packet as per the host message specifications (See [Appendix H](#_Annexure)) 2. Checks the Terminal totals should get updated by the transaction amount 3. Checks the Terminal is sending all the mandatory fields to the host 4. Checks for the Invoice no and Stan increment 5. Checks receipt contents: should print Merchant headers,Txn time, Txn date, MID, TID, Batch No, Invoice No,Txn Name,Card No, Card type, Exp Date, Card-holder’s Name, Amount, Auth Code, RRN, Disclaimer, Signature space and footer correctly. |
| **Alternate Flow** | | | |
| **Step** | **Scenario** | | **User/System Action** |
|  | User tries to swipes the card which is not configured in the card range | | Terminal will not proceed with the transaction and display appropriate error message to the user |
|  | User tries to enter the card number which is not configured in the card range | | Terminal will not proceed with the transaction and display appropriate error message to the user |
|  | User enters a card number with invalid Luhn (Invalid Card) | | Terminal will check the Luhn as per the defined logic. It will not proceed with the transaction and will display the message 'Luhn check Failed' |
|  | User swipes an expired card | | Terminal will read the card details from mag stripe, verifies the card number and the expiry date.  Terminal will not proceed with the transaction and will display the message 'Expired Card' |
|  | User enters a card number entered with expiry date less than the current date | | Terminal will verify the card number and the expiry date.  Terminal will not proceed with the transaction and will display the message 'Expired Card' |
|  | User enters a card number entered with expiry date in invalid format | | Terminal will verify the card number and the expiry date.  Terminal will not proceed with the transaction and display message 'Expired Card' |
|  | User swipes a card swiped and enters an invalid amount | | Terminal will read the card details from mag stripe and verify the following:   * Card number * Expiry date * Amount   Terminal will not proceed with the transaction and will display the message 'Invalid Amount' |
|  | User enters a card number entered with an invalid amount | | Terminal will verify the following:   * Card number * Expiry date * Amount   Terminal will not proceed with the transaction and display message 'Invalid Amount' |
|  | User swipes a card and presses the cancel button | | Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User swipes a card, enters the amount, auth code and then presses the cancel button | | Terminal will read the card details from mag stripe; verify the card number, amount and the expiry date.  Terminal will not proceed with the transaction and reset itself to idle mode  At host, the invoice no. will not be incremented |
|  | User enters the Card no., expiry date and then presses the cancel button | | Terminal will not proceed with the transaction and reset itself to idle mode  At host, the invoice no. will not be incremented |
| **Business Rules** | | | |
|  | Offline transaction is not allowed for Cash Back and Purchase with Cash back transactions | | |
|  | Cashback amount can be entered only in the multiples of hundred | | |
|  | Following is the Accounting Entry for Cash@POS incentive transactions:   |  |  | | --- | --- | | **DEBIT** | **CREDIT** | | Debit Cash@POS Interchange Account | Credit ME A/c  Credit Cash@POS Incentive Account | | | |
|  |  | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message/Action** |
|  | Connection timeout between the terminal and host | | Appropriate error message will be displayed to the user on the terminal screen |

#### Use Case: UC-Offline Sale Transaction-005

|  |  |  |  |
| --- | --- | --- | --- |
| Use Case 005: Offline Sale Transaction | | | |
| **Description** | | This use case describes the offline transaction that is used on the POS machine to perform a normal sale in offline scenario | |
| **Actors** | | Terminal, Merchant, Bank | |
| **Pre-Condition** | | Rev file should be downloaded onto the terminal and the parameters are initialized | |
| **Post-Condition** | | Chargeslip is printed after successful transactions | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | **Card Swipe:**   1. User selects the Sale option on the EDC machine 2. User swipes the card 3. User enters the amount and the Auth code | | 1. The terminal system will read the card details from magnetic strip. 2. It will verify the card number in the card range, Expiry date, Amount and the Auth code. It will dial the configured telephone number. 3. Terminal will display the Approval code after successful transactions 4. Terminal will print the receipt/charge slip after the transaction |
|  | **Manual Entry:**   1. User selects the Offline Sale option on the EDC machine 2. User enters the card number 3. User enters the expiry date 4. User enters the amount and the auth code | | 1. Terminal will verify the Luhn and the card number in Card Range 2. Terminal will verify the Expiry date, Amount and the Auth code 3. Terminal will print the receipt/charge slip after the transaction |
|  | **EMV:**   1. User selects the Sale option on the EDC machine 2. User inserts the card 3. User enters the amount | | 1. The terminal will read the card details from chip 2. It will verify the Luhn and the card number in Card Range 3. Terminal will verify the expiry date and the amount 4. Terminal will display the Approval code after successful transactions 5. Terminal will print the receipt/charge slip after the transaction |
|  |  | | **Host**:   1. Host checks whether the terminal is sending the offline sale (swipe/manual/EMV) request packet as per the host message specifications (See [Appendix H](#_Annexure)) 2. Checks the Terminal totals should get updated by the transaction amount 3. Checks the Terminal is sending all the mandatory fields to the host 4. Checks for the Invoice no and Stan increment 5. Check the approval code for offline sale (EMV) is all spaces. 6. Checks receipt contents as per specified format as given below: Merchant headers,Txn time, Txn date, MID, TID, Batch No, Invoice No,Txn Name,Card No, Card type, Exp Date, Amount, Auth Code, Disclaimer, Signature space and footer correctly. |
| **Alternate Flow** | | | |
| **Step** | **Scenario** | | **User/System Action** |
|  | User tries to swipes the card which is not configured in the card range | | Terminal will not proceed with the transaction and display appropriate error message to the user |
|  | User tries to enter the card number which is not configured in the card range | | Terminal will not proceed with the transaction and display appropriate error message to the user |
|  | User enters a card number with invalid Luhn (Invalid Card) | | Terminal will check the Luhn as per the defined logic. It will not proceed with the transaction and will display the message 'Luhn check Failed' |
|  | User swipes an expired card | | Terminal will read the card details from mag stripe, verifies the card number and the expiry date.  Terminal will not proceed with the transaction and will display the message 'Expired Card' |
|  | User enters a card number entered with expiry date less than the current date | | Terminal will verify the card number and the expiry date.  Terminal will not proceed with the transaction and will display the message 'Expired Card' |
|  | User enters a card number entered with expiry date in invalid format | | Terminal will verify the card number and the expiry date.  Terminal will not proceed with the transaction and display message 'Expired Card' |
|  | User swipes a card swiped and enters an invalid amount | | Terminal will read the card details from mag stripe and verify the following:   * Card number * Expiry date * Amount   Terminal will not proceed with the transaction and will display the message 'Invalid Amount' |
|  | User enters a card number entered with an invalid amount | | Terminal will verify the following:   * Card number * Expiry date * Amount   Terminal will not proceed with the transaction and display message 'Invalid Amount' |
|  | User swipes a card, enters the amount and an invalid auth code (i.e. Code more than the 6 digit's, Null, special Char's and zero) | | Terminal will read the card details from mag stripe and verify the following:   * Card number * Expiry date * Amount * Auth   Terminal will not proceed with the transaction |
|  | User enters the card number, enters the amount and an invalid auth code (i.e. Code more than the 6 digit's, Null, special Char's and zero | | Terminal will verify the following:   * Card number * Expiry date * Amount * Auth   Terminal will not proceed with the transaction |
|  | User swipes a card and presses the cancel button | | Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User swipes a card, enters the amount, auth code and then presses the cancel button | | Terminal will read the card details from mag stripe; verify the card number, amount and the expiry date.  Terminal will not proceed with the transaction and reset itself to idle mode  At host, the invoice no. will not be incremented |
|  | User enters the Card no., expiry date and then presses the cancel button | | Terminal will not proceed with the transaction and reset itself to idle mode  At host, the invoice no. will not be incremented |
|  | User swipes the card, enters the amount, auth code and presses the cancel button while printing | | Terminal will read the card details from mag stripe; It will verify the card number, expiry date and the amount.  Terminal will not take the cancel command while printing. It will proceed with the transaction  Host will check the following:   * Request packet * Terminal totals * Invoice no & Stan no. * Receipt contents * Auth Code |
| **Business Rules** | | | |
|  | Offline transaction is not allowed for Cash Back and Purchase with Cash back transactions | | |
|  | Expiry Date on the card should not be less than the current date | | |
|  | The Terminal totals should get updated by the transaction amount | | |
|  | If a particular card is not configured in the card range then the terminal should not proceed with the transaction | | |
|  | The Auth code should be padded with trailing spaces, if it has less than six digits. | | |
|  | The Off-Line transaction should be sent as a request to the host immediately and should not wait for the next online transaction. | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message/Action** |
|  | Connection timeout between the terminal and host | | Appropriate error message will be displayed to the user on the terminal screen |

#### Use Case: UC-Refund-006

|  |  |  |  |
| --- | --- | --- | --- |
| Use Case 006: Refund Transaction | | | |
| **Description** | | This use case describes the refund transaction that happens in the POS terminal | |
| **Actors** | | Terminal, Host | |
| **Pre-Condition** | | Rev file should be downloaded onto the terminal and the parameters are initialized | |
| **Post-Condition** | | Chargeslip is printed after successful transactions | |
| **Main Flow** | | | |
| **Step** | **Scenario** | | **User/System Action** |
|  | **Card Swipe:**   1. User selects the Refund option on the EDC machine 2. User swipes the card 3. User enters the amount | | 1. The terminal system will read the card details from magnetic strip. 2. It will verify the card number in the card range, Expiry date and the Amount. It will dial the configured telephone number. 3. Terminal will display the Approval code after successful transactions 4. Terminal will print the receipt/charge slip after the transaction |
|  | **Manual Entry:**   1. User selects the Refund option on the EDC machine 2. User enters the card number 3. User enters the expiry date 4. User enters the amount | | 1. Terminal will verify the Luhn and the card number in Card Range 2. Terminal will verify the Expiry date, Amount 3. Terminal will display the Approval code after successful transactions 4. Terminal will print the receipt/charge slip after the transaction |
|  | **EMV:**   1. User selects the Refund option on the EDC machine 2. User inserts the card in the chip reader 3. User enters the amount | | 1. The terminal will read the card details from the chip 2. It will verify the card number in Card Range 3. Terminal will verify the expiry date and the amount 4. Terminal will display the Approval code after successful transactions 5. Terminal will print the receipt/charge slip after the transaction |
|  |  | | **Host**:   1. Host checks whether the terminal is sending the Refund (swipe/manual/EMV) request packet as per the host message specifications (See [Appendix H](#_Annexure)) 2. Checks the Terminal totals should get updated by the transaction amount 3. Checks the Terminal is sending all the mandatory fields to the host 4. Checks for the Invoice no and Stan increment 5. Checks receipt contents as per specified format as given below: Merchant headers,Txn time, Txn date, MID, TID, Batch No, Invoice No,Txn Name,Card No, Card type, Exp Date, Amount, Auth Code, Disclaimer, Signature space and footer correctly. |
| **Alternate Flow** | | | |
| **Step** | **Scenario** | | **User/System Action** |
|  | User selects the Refund option and tries to swipe the card which is not configured in the card range | | Terminal will not proceed with the transaction and display appropriate error message to the user |
|  | User selects the Refund option and tries to enter the card number which is not configured in the card range | | Terminal will not proceed with the transaction and display appropriate error message to the user |
|  | User selects the Refund option and enters a card number with invalid Luhn (Invalid Card) | | Terminal will check the Luhn as per the defined logic. It will not proceed with the transaction and will display the message 'Luhn check Failed' |
|  | User selects the Refund option and swipes an expired card | | Terminal will read the card details from mag stripe, verifies the card number and the expiry date.  Terminal will not proceed with the transaction and will display the message 'Expired Card' |
|  | User selects the Refund option and a card number is entered with expiry date less than the current date | | Terminal will verify the card number and the expiry date.  Terminal will not proceed with the transaction and will display the message 'Expired Card' |
|  | User selects the Refund option and enters a card number with expiry date in invalid format | | Terminal will verify the card number and the expiry date.  Terminal will not proceed with the transaction and display message 'Expired Card' |
|  | User swipes a card swiped and enters an invalid amount | | Terminal will read the card details from mag stripe and verify the following:   * Card number * Expiry date * Amount   Terminal will not proceed with the transaction and will display the message 'Invalid Amount' |
|  | User enters a card number with an invalid amount | | Terminal will verify the following:   * Card number * Expiry date * Amount   Terminal will not proceed with the transaction and display message 'Invalid Amount' |
|  | User swipes a card and presses the cancel button | | Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User swipes a card, enters the amount and then presses the cancel button | | Terminal will read the card details from mag stripe; verify the card number, amount and the expiry date.  Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User enters the Card no., expiry date and then presses the cancel button | | Terminal will not proceed with the transaction and reset itself to idle mode |
|  |  | |  |
| **Business Rules** | | | |
|  | Expiry Date on the card should not be less than the current date | | |
|  | The Terminal totals should get updated by the transaction amount | | |
|  | In case of online transaction – Manual/EMV, the terminal verifies the Luhn | | |
|  | If a particular card is not configured in the card range then the terminal should not proceed with the transaction | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Connection timeout between the terminal and host | | Appropriate error message will be displayed to the user on the terminal screen |

#### Use Case: UC-Void Sale-007

|  |  |  |  |
| --- | --- | --- | --- |
| Use Case 007: Void Sale Transaction | | | |
| **Description** | | This use case describes the void transaction that is used to inform the host that a sale / refund transaction previously performed at the terminal has been cancelled. | |
| **Actors** | | Terminal, Host | |
| **Pre-Condition** | | Rev file should be downloaded onto the terminal and the parameters are initialized | |
| **Post-Condition** | | Chargeslip is printed after successful transactions | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | **Terminal Input:**   1. User selects the Void option on the EDC machine 2. User enters the Invoice no. of an online/offline/EMV Sale transaction 3. User enters the Invoice No of an online/offline/EMV Refund Transaction | | **Terminal Output:**   1. The terminal system will verify the invoice no. 2. The terminal will display transaction type and amount 3. Terminal will display approval code 4. Terminal will print the receipt as per the format |
|  |  | | **Host**:   1. Host checks whether the terminal is sending the Void Sale/Refund (swipe/manual/EMV) request packet as per the host message specifications (See [Appendix H](#_Annexure)) 2. Checks the Terminal totals should get updated by the transaction amount 3. Checks the Invoice no. is same as of the original sale 4. Checks for the Invoice no and Stan increment 5. Checks the Invoice no, POS entry mode, POS condition code and auth id should be same as of the original refund transaction. 6. Checks receipt contents as per specified format as given below: Merchant headers,Txn time, Txn date, MID, TID, Batch No, Invoice No,Txn Name,Card No, Card type, Exp Date, Amount, Auth Code, Disclaimer, Signature space and footer correctly. |
| **Alternate Flow** | | | |
| **Step** | **Scenario** | | **User/System Action** |
|  | User enters Invoice No of a transaction that is already settled | | Terminal will verify the Invoice no. Terminal will not proceed with the transaction and display appropriate error message to the user |
|  | User enters Invoice No more than the running invoice no | | Terminal will verify the Invoice no. Terminal will not proceed with the transaction and display appropriate error message to the user |
|  | User enters the Invoice no other than the Online sale, Offline sale, Offline Adjust and Refund transaction | | Terminal will verify the Invoice no. Terminal will not proceed with the transaction and display message the error message 'Wrong Invoice No' |
|  | User enters Invoice No of a Voided transaction | | Terminal will verify the Invoice no. It will not proceed with the transaction and will display the message 'Already Voided' |
|  | User enters the Invoice no. and presses the cancel button | | Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User enters the Invoice no. and presses the cancel button after the display of transaction details | | Terminal will verify the Invoice no.  Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User enters the Invoice no. and presses the cancel button wile processing void transaction | | Terminal will verify the Invoice no. Terminal will not take the cancel command and will proceed with the transaction.  Host will check the following:   * Void Sale Request packet * Terminal totals * Invoice no is same as of the original sale * Receipt contents |
| **Business Rules** | | | |
|  | The Terminal totals should get updated by the transaction amount | | |
|  | If transaction is offline void, then the transaction is sent to the host by piggy backing along with next online transaction. In case of online void the transaction is sent to the host immediately. | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Connection timeout between the terminal and host | | Appropriate error message will be displayed to the user on the terminal screen |

#### Use Case: UC-Tip Adjust transaction-008

|  |  |  |  |
| --- | --- | --- | --- |
| Use Case 008: Tip Adjust Transaction | | | |
| **Description** | | This use case describes the Tip Adjust transaction that is used to notify the host that there has been an addition to the amount of a previous transaction. | |
| **Actors** | | Terminal, Host | |
| **Pre-Condition** | | Rev file should be downloaded onto the terminal and the parameters are initialized | |
| **Post-Condition** | | Chargeslip is printed after successful transactions | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | **Terminal Input:**   1. User selects the Tip-Adjust option on the EDC machine 2. User enters the valid Invoice No of an Online/Offline/EMV Transaction 3. User enters a Tip Amount   **Note:** For the Invoice no. of an offline transaction which has been sent/not sent to the host, will follow the same user action steps defined as above | | **Terminal Output:**   1. The terminal system will verify the invoice no. and the tip amount 2. The terminal will display transaction type and amount 3. Terminal will display approval code of original transaction 4. Terminal will print the receipt as per the format |
|  |  | | **Host**:   1. Host checks whether the terminal is sending the Tip-Adjust Sale request packet as per the host message specifications (See [Appendix H](#_Annexure)) 2. Checks the Terminal totals should get updated by the transaction amount 3. Checks the terminal is sending all the mandatory fields mentioned in the spec to the host. 4. Checks the Invoice no, STAN, time, date and response code same as original transaction. 5. Checks receipt contents as per specified format as given below: Merchant headers,Txn time, Txn date, MID, TID, Batch No, Invoice No,Txn Name,Card No, Card type, Exp Date, Amount, Auth Code, Disclaimer, Signature space and footer correctly. |
| **Alternate Flow** | | | |
| **Step** | **Scenario** | | **User/System Action** |
|  | User enters Invoice No of a transaction that is already settled | | Terminal will verify the Invoice no. Terminal will not proceed with the transaction and display message the error message 'Wrong Invoice No' |
|  | User enters Invoice No more than the running invoice no | | Terminal will verify the Invoice no. Terminal will not proceed with the transaction and display message the error message 'Wrong Invoice No' |
|  | User enters the Invoice no other than the Credit Sale transaction | | Terminal will verify the Invoice no. Terminal will not proceed with the transaction and display message the error message 'Wrong Invoice No' |
|  | User enters Invoice No of a Voided transaction | | Terminal will verify the Invoice no. It will not proceed with the transaction and will display the message 'Txn Already Voided' |
|  | User enters Invoice No of already Tip-Adjusted transaction | | Terminal will verify the Invoice no. It will not proceed with the transaction and will display the message 'Txn not allowed’ |
|  | User enters the Invoice no. and enters an invalid amount | | Terminal will verify the Invoice no and the tip-amount. It will not proceed with the transaction and will display the message 'Invalid Amount’ |
|  | User enters the Invoice no. and presses the cancel button | | Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User enters the Invoice no. and presses the cancel button after entering a new amount | | Terminal will verify the Invoice no. Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User enters the Invoice no. and presses the cancel button wile processing the Tip-Adjust transaction | | Terminal will verify the Invoice no. Terminal will not take the cancel command and will proceed with the transaction.  Host will check the following:   * Tip-Adjust Sale Request packet * Terminal totals * Invoice no and STAN will not be incremented * Receipt contents |
| **Business Rules** | | | |
|  | The Terminal totals should get updated by the transaction amount | | |
|  | TIP Adjust is not allowed for Purchase with Cash Back transactions and Cash back transactions. | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Connection timeout between the terminal and host | | Appropriate error message will be displayed to the user on the terminal screen |

#### Use Case: UC-Pre-Auth-009

|  |  |  |  |
| --- | --- | --- | --- |
| Use Case 009: Pre-Auth Transaction | | | |
| **Description** | | This use case describes how a transaction is stored in the pre-authorized transactions batch in the terminal when approved. | |
| **Actors** | | Terminal, Host | |
| **Pre-Condition** | | Rev file should be downloaded onto the terminal and the parameters are initialized | |
| **Post-Condition** | | Chargeslip is printed after successful transactions | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | **Card Swipe:**   1. User selects the Pre-Auth on the EDC machine 2. User swipes the card 3. User enters the amount | | 1. The terminal system will read the card details from magnetic strip. 2. It will verify the card number in the card range, Expiry date and the Amount. It will dial the configured telephone number. 3. Terminal will display the Approval code after successful transactions 4. Terminal will print the receipt as per the format 5. It will store the transaction in a separate batch |
|  | **Manual Entry:**   1. User selects the Pre-Auth option on the EDC machine 2. User enters the card number 3. User enters the expiry date 4. User enters the amount | | 1. Terminal will verify the Luhn and the card number in Card Range 2. Terminal will verify the Expiry date, Amount. It will dial the configured telephone number. 3. Terminal will display the Approval code after successful transactions 4. Terminal will print the receipt as per the format 5. It will store the transaction in a separate batch |
|  | **EMV:**   1. User selects the Pre-Auth option on the EDC machine 2. User inserts the card in the chip reader 3. User enters the amount | | 1. The terminal will read the card details from the chip 2. It will verify the card number in Card Range 3. Terminal will verify the expiry date and the amount. It will dial the configured telephone number. 4. Terminal will display the Approval code after successful transactions 5. Terminal will print the receipt as per the format 6. It will store the transaction in a separate batch |
|  |  | | **Host**:   1. Host checks whether the terminal is sending the Pre-Auth (swipe/manual/EMV) request packet as per the host message specifications (See [Appendix H](#_Annexure)) 2. Checks the Terminal totals shouldn’t get updated by the transaction amount 3. Checks the Terminal is sending all the mandatory fields to the host 4. Checks for the Invoice no and Stan increment 5. Check the POS condition code is 06 |
| **Alternate Flow** | | | |
| **Step** | **Scenario** | | **User/System Action** |
|  | User selects the Pre-Auth option and tries to swipe the card which is not configured in the card range | | Terminal will not proceed with the transaction and display appropriate error message to the user |
|  | User selects the Pre-Auth option and tries to enter the card number which is not configured in the card range | | Terminal will not proceed with the transaction and display appropriate error message to the user |
|  | User selects the Pre-Auth option and enters a card number with invalid Luhn (Invalid Card) | | Terminal will check the Luhn as per the defined logic. It will not proceed with the transaction and will display the message 'Luhn check Failed' |
|  | User selects the Pre-Auth option and swipes an expired card | | Terminal will read the card details from mag stripe, verifies the card number and the expiry date.  Terminal will not proceed with the transaction and will display the message 'Expired Card' |
|  | User selects the Pre-Auth option and a card number is entered with expiry date less than the current date | | Terminal will verify the card number and the expiry date.  Terminal will not proceed with the transaction and will display the message 'Expired Card' |
|  | User selects the Pre-Auth option and enters a card number with expiry date in invalid format | | Terminal will verify the card number and the expiry date.  Terminal will not proceed with the transaction and display message 'Expired Card' |
|  | User swipes a card swiped and enters an invalid amount | | Terminal will read the card details from mag stripe and verify the following:   * Card number * Expiry date * Amount   Terminal will not proceed with the transaction and will display the message 'Invalid Amount' |
|  | User enters a card number with an invalid amount | | Terminal will verify the following:   * Card number * Expiry date * Amount   Terminal will not proceed with the transaction and display message 'Invalid Amount' |
|  | User swipes a card and presses the cancel button | | Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User swipes a card, enters the amount and then presses the cancel button | | Terminal will read the card details from mag stripe; verify the card number, amount and the expiry date.  Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User enters the Card no., expiry date and then presses the cancel button | | Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User swipes the card, enters the amount and presses the cancel button before connecting to host | | Terminal will read the card details from mag stripe; verify the card number, expiry date and amount  Terminal will not proceed with the transaction and reset itself to idle mode. |
|  | User swipes the card, enters the amount and presses the cancel button after receiving the approval code | | Terminal will read the card details from mag stripe; verify the card number, expiry date and amount  Terminal will not take the cancel command after receiving the approval code. It will proceed with the transaction  Host will check the following:   * Pre-Auth (Swipe) request packet * Terminal totals |
|  | User swipes the card, enters the amount and presses the cancel button while printing | | Terminal will read the card details from mag stripe; verify the card number, expiry date and amount  Terminal will not take the cancel command after receiving the approval code. It will proceed with the transaction  Host will check the following:   * Pre-Auth (Swipe) request packet * Terminal totals * Check for Invoice no. and STAN increment |
|  | User selects the settlement option after Pre-Auth transaction | | Terminal will not send the pre-auth transaction to the host |
|  | User selects the batch delete option after Pre-Auth transaction | | Terminal will not delete the pre-auth transaction |
| **Business Rules** | | | |
|  | Expiry Date on the card should not be less than the current date | | |
|  | The Terminal totals should get updated by the transaction amount | | |
|  | In case of online transaction – Manual/EMV, the terminal verifies the Luhn | | |
|  | If a particular card is not configured in the card range then the terminal should not proceed with the transaction | | |
|  | A Pre-authorized transaction is stored as a separate batch in the terminal when approved. This batch is not settled with the Host. When Sale completion transaction is undertaken for a pre-authorized transaction, the same is transferred from Pre-Authorized transactions batch to the regular transactions batch in the terminal. | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Connection timeout between the terminal and host | | Appropriate error message will be displayed to the user on the terminal screen |

#### Use Case: UC-Sale Completion-010

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Use Case 010: Sale Completion Transaction | | | | | |
| **Description** | | | This use case describes the Sale Completion transaction that is used to complete a Pre-Authorize transaction when the exact amount is known. | | |
| **Actors** | | | Terminal, Host | | |
| **Pre-Condition** | | | Rev file should be downloaded onto the terminal and the parameters are initialized | | |
| **Post-Condition** | | | Chargeslip is printed after successful transactions | | |
| **Main Flow** | | | | | |
| **Step** | | **User Action** | | | **System Action** |
|  | | **Terminal Input:**   1. User selects the Sale Completion option on the EDC machine 2. User can either swipe the card or enter the Invoice no. and the amount 3. If the user enters the invoice no., then he will select the type of card – Credit/Debit/EUR/USD | | | **Terminal Output:**   1. The terminal system will verify the Invoice no. and the Amount 2. Terminal will print the receipt as per the format 3. It will store the transaction in the current batch 4. Terminal will send the sale completion transaction to the host as piggyback transaction |
|  | |  | | | **Host**:   1. Host checks whether the terminal is sending the Sale Completion transaction(swipe/manual/EMV) request packet as per the host message specifications (See [Appendix H](#_Annexure)) 2. Checks the Terminal totals should get updated by the transaction amount 3. Checks the Terminal is sending all the mandatory fields to the host 4. Checks the Invoice no is not incremented 5. Checks the Stan increment |
| **Alternate Flow** | | | | | |
| **Step** | | **User Action** | | | **System Action** |
|  | | User selects the specified key for sale completion and enters Invoice No of a pre-auth transaction for which Sale Completion is already done. | | | Terminal will verify the invoice no. Terminal will not proceed with the transaction and display the message 'Wrong Invoice No' to the user |
|  | | User selects the specified Key for sale completion and enters Invoice No more than the running invoice no | | | Terminal will not proceed with the transaction and display the message 'Wrong Invoice No' to the user |
|  | | User selects the specified Key for sale completion and enters Invoice No other than the pre-auth transaction | | | Terminal will not proceed with the transaction and display the message 'Wrong Invoice No' to the user |
|  | | User selects the specified Key for sale completion and enters Invoice no., invalid amount | | | Terminal will verify the invoice no. and the amount.  Terminal will not proceed with the transaction and will display the message 'Invalid Amount' |
|  | | User selects the specified Key for sale completion, enters Invoice no. and presses the cancel button | | | Terminal will not proceed with the transaction and resets itself to idle mode |
|  | | User selects the specified Key for sale completion, enters Invoice No and amount and then presses the cancel button | | | Terminal will verify the invoice no.  Terminal will not proceed with the transaction and reset itself to idle mode |
|  | | User selects the specified Key for sale completion, enters Invoice No, enters Amount and presses the cancel button while printing | | | Terminal will verify the invoice no. and amount  Terminal will proceed with the transaction  Host will check the following:   * Sale Completion transaction request packet * Terminal totals * Check for Invoice no. and STAN increment * POS condition code |
| **Exceptional Flow** | | | | | |
| **Sr. No.** | **Exception** | | | **Error Message** | |
| 1 | Connection timeout between the terminal and host | | | Appropriate error message will be displayed to the user on the terminal screen | |

#### Use Case: UC-Normal Settlement Transaction-011

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Use Case 011: Normal Settlement | | | | |
| **Description** | | This use case describes the execution of settlement transaction | | |
| **Actors** | | Terminal, Host | | |
| **Pre-Condition** | | Rev file should be downloaded onto the terminal and the parameters are initialized | | |
| **Post-Condition** | | Charge slip is printed after successful transactions | | |
| **Main Flow** | | | | |
| **Step** | **User Action** | | | **System Action** |
|  | **Terminal Input:**  User selects the specified key for Settlement on the EDC machine | | | **Terminal Output:**   1. The terminal system will verify the batch and totals 2. It will dial the configured telephone no to the host 3. Terminal will send the pending reversal (If any) to the Host before sending any to the request. 4. Terminal will send all the pending advices (if any) to the host 5. Terminal will display ‘settle success’ after getting approval (Response Code '00') from host. 6. Terminal will verify the Response Code received from the host 7. Terminal will print the settlement receipt after successful settlement. 8. Batch will get cleared from terminal after successful settlement |
|  |  | | | **Host**:   1. Host checks whether the terminal is sending the Normal settlement request packet as per the host message specifications (See [Appendix H](#_Annexure)) 2. Checks the Terminal totals should get updated by null 3. Checks the Batch no., Invoice no. and Stan increment 4. Checks receipt contents as per specified format as given below: Merchant headers,Txn time, Txn date, MID, TID, Batch No, Report Name , Invoice number , Card Type, Txn Name, Card No., Exp Date, Auth code, Amount, ( for each txn ) , the Totals : Sales , Void-Sales , Refunds , Void-Refunds , Total Amount 5. Checks that the version number sent in the settlement packet is matching the software version which is displayed on the terminal ( if displayed on the terminal ) 6. Checks whether the total number of Debit txns is total number effective Sales txns ( i.e.Sales - Void Sales ) and the total number of Credit txns is the total number of effective Refunds txns ( i.e. Refunds - Void Refunds ). 7. Verifies the EE counter. This should be equal to the number of txns which exceed the set time limit. |
| **Alternate Flow** | | | | |
| **Step** | **User Action** | | | **System Action** |
|  | User selects the specified key for settlement | | | Terminal will verify the batch. Terminal will not dial the host if Batch doesn’t exist and will display the message ‘Batch Empty’ |
|  | User selects the specified Key for settlement | | | Terminal will verify the batch and the totals. It will not dial the host if Nett totals are Null and will display the message ‘Null totals’ |
|  | User selects the specified Key for settlement | | | Terminal will verify the batch and the totals. It will dial the host and verifies if the response code is other than ‘00’.  Terminal will display appropriate message if response code is other than approval. Terminal will retain the Current batch totals and details. |
|  | User selects the specified Key for settlement | | | Terminal will verify the batch and the totals. It will dial the host and verifies if the response code is other than ‘95’.  Terminal will retain the Current batch totals and details. It will initiate the Batch upload |
|  | Verify the response packet for settlement request for a successful settlement | | | 1. Based on the data received in response packet, terminal will print the message on the transaction slip as "Pls. keep the terminal connected as there is a parameter download at HH:MM " 2. The terminal will dial out to the TMS server for application and host for parameter downloads based on the flag value. 3. Also this dialing will happen as per the time received for download (should start at the specified time automatically). |
| **Business Rules** | | | | |
|  | Terminal should not initiate batch settlement if there are reversal or pre-auth pending | | | |
|  | Terminal should print the date and time on the charge slip as received from the host. | | | |
| **Exceptional Flow** | | | | |
| **Sr. No.** | **Exception** | | **Error Message** | |
|  | Connection timeout between the terminal and host | | | Appropriate error message will be displayed to the user on the terminal screen |

#### Use Case: UC-Batch Upload-012

|  |  |  |  |
| --- | --- | --- | --- |
| Use Case 012: Batch Upload | | | |
| **Description** | | This use case describes the batch upload process after an unsuccessful settlement attempt that happens in the terminal | |
| **Actors** | | Terminal, Host | |
| **Pre-Condition** | | Rev file should be downloaded onto the terminal and the parameters are initialized | |
| **Post-Condition** | | Chargeslip is printed after successful transactions | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | **Terminal:**   1. Terminal will verify the response code ‘95’ received in the normal settlement response 2. Terminal will initiate the Batch Settlement 3. Terminal will start sending all the valid Sale and Refund transactions to the host one by one. 4. Terminal will not send Void and adjust transaction separately. 5. Terminal will send the Settlement request to the Host | | **Host:**   1. Host will check the batch upload request packet as per the host message specification. (See [Appendix H](#_Annexure)) 2. Checks for STAN increment 3. Checks the Batch No and Invoice no. are not incremented. Date & Time must be of the original transaction. |
| **Business Rules** | | | |
|  | Batch Upload is initiated only in the case when the Normal Settlement response = ‘95’ | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Connection timeout between the terminal and host | | Appropriate error message will be displayed to the user on the terminal screen |

#### Use Case: UC-Settlement after Upload-013

|  |  |  |  |
| --- | --- | --- | --- |
| Use Case 013: Settlement after upload | | | |
| **Description** | | This use case describes the settlement after upload transaction | |
| **Actors** | | Terminal, Host | |
| **Pre-Condition** | | Rev file should be downloaded onto the terminal and the parameters are initialized | |
| **Post-Condition** | | Chargeslip is printed after successful transactions | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | **Terminal Input:**   1. User initiates Normal Settlement 2. Upload is completed after total mismatch | | **Terminal Output:**   1. The terminal will dial the host 2. It will verify the response code received from host for normal settlement 3. Terminal will display ‘settle success’ after getting approval from host 4. Terminal will print the settlement receipt after successful settlement 5. Batch will get cleared from terminal after successful settlement |
|  |  | | **Host**:   1. Host checks whether the terminal is sending the Upload settlement request packet as per the host message specifications (See [Appendix H](#_Annexure)) 2. Checks the Terminal totals should get updated by null 3. Checks the Batch no. and Stan increment 4. Checks receipt contents as per specified format 5. Verify the EE counter. This should be equal to the number of txns which exceed the set time limit |
| **Alternate Flow** | | | |
| **Step** | **Scenario** | | **User/System Action** |
|  | User selects the specified Key for settlement | | Terminal will verify the batch and the totals. It will dial the host and verifies if the response code is other than ‘00’.  Terminal will display appropriate message if response code is other than approval. Terminal will retain the Current batch totals and details. |
|  | User selects the specified Key for settlement | | Terminal will verify the batch and the totals. It will dial the host and verifies if the response code is ‘95’.  Terminal will display the message ‘Retry Settlement’ and it shouldn’t initiate the Batch upload |
|  | Verify the response packet for settlement request for a successful settlement | | 1. Based on the data received in response packet, terminal will print the message on the transaction slip as "Pls. keep the terminal connected as there is a parameter download at HH:MM " 2. The terminal will dial out to the TMS server for application and host for parameter downloads based on the flag value. 3. Also this dialing will happen as per the time received for download (should start at the specified time automatically). |
| **Business Rules** | | | |
|  | Terminal should print the date and time on the charge slip as received from the host. | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Connection timeout between the terminal and host | | Appropriate error message will be displayed to the user on the terminal screen |

#### Use Case: UC-Balance Inquiry (Debit Transaction)-014

|  |  |  |  |
| --- | --- | --- | --- |
| Use Case 014: Key Exchange | | | |
| **Description** | | This use case describes the balance inquiry transaction that is used to obtain the balance of a debit card. | |
| **Actors** | | Terminal, Host | |
| **Pre-Condition** | | Rev file should be downloaded onto the terminal and the parameters are initialized | |
| **Post-Condition** | | The transaction response is displayed on the PIN pad device. | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | **Swipe card:**   1. User selects the ‘Balance Enquiry’ option on the EDC machine 2. User swipes the card 3. Selects the Account Type – Savings/Checking/Current 4. Enters the PIN | | 1. Terminal will read the card details from mag stripe 2. It will verify the following:  * Card number in Card Range * Expiry date * PIN  1. Terminal will dial the host 2. It will display Balance Amount and print the receipt as per specified format (If implemented)   **Host**:   1. Host checks whether the terminal is sending the Balance Enquiry request packet as per host message specification. (See [Appendix H](#_Annexure)) 2. Checks for the Invoice no should not get increment 3. Checks for Stan increment |
|  | **EMV:**   1. User selects the ‘Balance Enquiry’ option on the EDC machine 2. User swipes the card 3. Selects the Account – Saving/Checking/Credit 4. Enters the PIN | | 1. Terminal will read the card details from mag stripe 2. It will verify the following:  * Card number in Card Range * Expiry date * PIN  1. Terminal will dial the host 2. It will display Balance Amount and print the receipt as per   **Host**:   1. Host checks whether the terminal is sending the Balance Enquiry request packet as per host message specification. (See [Appendix H](#_Annexure)) 2. Checks for the Invoice no should not get increment 3. Checks for Stan increment 4. Check the terminal is sending all the mandatory tags in field 55 5. Check the POS entry mode is 051 6. Check the proc code is '313000' |
| **Alternate Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | User selects the Balance Enquiry option and tries to enter the card no. manually | | Terminal will not allow the transaction |
|  | User selects the Balance Enquiry option on the EDC machine and tries to swipe a card that is not configured in the card range | | Terminal will not proceed with the transaction and display appropriate message |
|  | User selects the Balance Enquiry option on the EDC machine and tries to swipe an expired card | | Terminal will not proceed with the transaction and display message 'Expired Card' |
|  | User selects the Balance Enquiry option and swipes the card, selects the account and enters an invalid PIN | | Terminal will not proceed with the transaction |
|  | User swipes a card and presses the cancel button | | Terminal will not proceed with the transaction and resets itself to idle mode |
|  | User swipes the card, selects the account and presses the cancel button | | Terminal will not proceed with the transaction and resets itself to idle mode |
|  | User swipes the card, selects the account and presses the cancel button at PIN entry prompt | | Terminal will not proceed with the transaction and resets itself to idle mode |
|  | User swipes the card, selects the account, enters the PIN and presses the cancel button before connecting to the host | | Terminal will not proceed with the transaction and resets itself to idle mode |
|  | User swipes the card, selects the account, enters the PIN and presses the cancel button after receiving the approval code | | Terminal will not take the cancel command after receiving the approval code. Terminal will proceed with the transaction. |
|  | User swipes the card, selects the account and presses the cancel button while printing | | Terminal will not take the cancel command while printing. Terminal will proceed with the transaction. |
|  | User swipes/inserts a damaged chip card | | Terminal will not proceed with the transaction and will display appropriate error message |
| **Business Rules** | | | |
|  | Balance Inquiry is supported only for Maestro Debit transactions, and not for other payment applications | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Connection timeout between the terminal and host | | Appropriate error message will be displayed to the user on the terminal screen |

#### Use Case: UC-Debit Sale (Online) Transaction-015

|  |  |  |  |
| --- | --- | --- | --- |
| Use Case 015: Online Sale | | | |
| **Description** | | This use case describes the online sale transaction that happens in the terminal using a debit card | |
| **Actors** | | Terminal, Merchant, Bank | |
| **Pre-Condition** | | Rev file should be downloaded onto the terminal and the parameters are initialized | |
| **Post-Condition** | | Chargeslip is printed after successful transactions | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
|  | **Card Swipe/EMV:**   1. User selects the Debit Sale option on the EDC machine 2. User swipes/inserts the card 3. User enters the amount 4. Selects the Account – Saving/Checking/Credit 5. Enter PIN | | 1. The terminal system will read the card details from magnetic strip. 2. It will verify the card number in the card range, Expiry date and the Amount. It will verify the PIN. 3. It will dial the configured telephone number. 4. Terminal will display the Approval code after successful transactions 5. Terminal will print the receipt as per the specified format |
|  |  | | **Host**:   1. Host checks whether the terminal is sending the Debit Sale request packet as per the host message specifications (See [Appendix H](#_Annexure)) 2. Checks the Terminal totals should get updated by the transaction amount 3. Checks the Terminal is sending all the mandatory fields to the host 4. Checks for the Invoice no and Stan increment for Debit batch. |
| **Alternate Flow** | | | |
| **Step** | **Scenario** | | **User/System Action** |
|  | User selects the Debit sale option and tries to enter the card no. manually | | Terminal will not allow manual entry |
|  | User tries to swipes the card which is not configured in the card range | | Terminal will not proceed with the transaction and display appropriate error message to the user |
|  | User swipes an expired card | | Terminal will read the card details from mag stripe, verifies the card number and the expiry date.  Terminal will not proceed with the transaction and will display the message 'Expired Card' |
|  | User swipes a card and enters an invalid amount | | Terminal will read the card details from mag stripe and verify the following:   * Card number * Expiry date * Amount   Terminal will not proceed with the transaction and will display the message 'Invalid Amount' |
|  | User swipes a card, enters the amount and an invalid PIN | | Terminal will not proceed with the transaction |
|  | User swipes a card and presses the cancel button | | Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User swipes a card, enters the amount and presses the cancel button | | Terminal will read the card details from mag stripe; verify the card number, expiry date and amount.  Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User swipes the card, enters amount, presses the cancel button after selecting the account | | Terminal will read the card details from mag stripe; It will verify the card number, expiry date and amount.  Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User swipes the card, selects the account and presses the cancel button at PIN entry prompt | | Terminal will not proceed with the transaction and reset itself to idle mode |
|  | User swipes the card, enters the amount and presses the cancel button before connecting to host | | Terminal will read the card details from mag stripe; verify the card number and expiry date  Terminal will not proceed with the transaction and reset itself to idle mode. At host, the invoice no. will not be incremented |
|  | User swipes the card, enters the amount and presses the cancel button after receiving the approval code | | Terminal will read the card details from mag stripe; verify the card number and expiry date  Terminal will not take the cancel command after receiving the approval code. It will proceed with the transaction  Host will check the following:   * Request packet * Terminal totals * Invoice no & Stan no. * Receipt contents |
|  | User enters the Card no., expiry date and then presses the cancel button | | Terminal will not proceed with the transaction and reset itself to idle mode.  At host, the invoice no. will not be incremented |
|  | User inserts a card, enters the amount and press cancel button before connecting to host | | Terminal will read the card details from the chip and verify the following:   * Card number * Expiry date * Amount   Terminal will not proceed with the transaction and reset itself to idle mode. Appropriate message will be displayed stating the transaction is declined. At host, the invoice no. will not be incremented. |
| **Business Rules** | | | |
|  | Expiry Date on the card should not be less than the current date | | |
|  | The Terminal totals should get updated by the transaction amount | | |
|  | In case of online transaction – Manual/EMV, the terminal verifies the Luhn | | |
|  | If a particular card is not configured in the card range then the terminal should not proceed with the transaction | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message/Action** |
|  | Connection timeout between the terminal and host | | Appropriate error message will be displayed to the user on the terminal screen |

## WL Host - Magnus

### PORT Mapping

Bank will procure a new Acquiring BIN with VISA and Rupay and shall procure a new ICA with MasterCard.

For Visa, a new acquiring BIN shall be procured and the Bank shall be provided a Port from the WL Pool of Station IDs. For MasterCard and Maestro acquiring, Bank shall procure a new ICA the same will be configured on WL MIP.

For Rupay Acquiring, Bank shall procure a new Acquiring BIN from NPCI and a dedicated Port & IP shall be allotted for the Bank.

### Formats Supported

The message formats mentioned are variable length, variable data content (ISO8583) - those that can be configured to carry different types of messages/values. The interface at Atos Worldline Host will be the server and the communication protocol used is TCP/IP. The host may send some additional fields in the response packet other than the ones specified in this document. In such cases, the External host should accept the response packet and ignore / not validate those additional fields.

The Atos Worldline External Host interface supports ISO8583-87 message formats. The interface will reformat the request before forwarding it to MasterCard & VISA Gateways or to the internal host module for authorisation. Reformatting will do the necessary changes to fields to generate a valid message type.

### Authorization Routing

* All Off-us transactions on VISA/Master/Maestro cards shall be routed through the bank port and RuPay transactions will be routed to NPCI.

### Data Field Definitions

#### PAN Number, Field 2

PAN number of the card used in the transaction. If the card is swiped, then this field is derived from the Track II data.

#### Processing Code, Field 3

The following is a table specifying the message type and processing code for each transaction type. In the Processing Code column, a = Account Selection.

|  |  |  |
| --- | --- | --- |
| **Transaction** | **Message Type** | **Processing Code** |
| Authorization  Balance Inquiry | 0100 | 00 a0 00  31 a0 00 |
| Sale | 0200 | 00 a0 00 |
| Reversal | 0400 | Same as original transaction |

#### Amount, Transaction, Field 4

The transaction amount is the total amount of the transaction. It can contain Tip or any Fee. Total length of the field is 12 digits

#### Transmission Date and Time, Field 7

This field contains the GMT time of the message transmission. Format of the field is MMDDhhmmss. Total length of the field is 10 digits

#### System trace Audit Number, Field 11

6 digit numeric field. Value can vary from 000001 to 999999.

#### Time Local transaction, Field 12

Field 12 contains the time the transaction takes place, expressed in the local time of the card acceptor location. Field format is HHMMSS where HH – Hour, MM – Minutes,

SS - Seconds

#### Date Local transaction, Field 13

Field 13 contains the month and day on which the cardholder originated the transaction. The date is in MMDD format, where: MM = month and DD = day

#### Date Expiration, Field 14

Field 14 contains the year and the month after which the card expires. The date is in

YYMM numeric format, where YY = year (00–99) and MM = month (01–12).

It is located in the track data or is entered

#### Merchant category code, Field 18

Field 18 contains a code describing the merchant’s type of business product or service, also known as the merchant category code (MCC). 4 digit ISO code of the MCC.

#### Acquiring Institution Country Code, Field 19

Field 19 contains a code that identifies the country of the acquiring institution for the merchant or ATM. 3 digit ISO code of the country.

#### POS Entry Mode, Field 22

The POS entry mode is used to indicate how the primary account number was entered into the terminal.

|  |  |  |  |
| --- | --- | --- | --- |
| Positions 1 and 2 | PAN entry mode | Position 3 | PIN entry capability |
| 00 | Unspecified | 0 | Unspecified |
| 01 | Manual | 1 | PIN entry capability |
| 02 | Magnetic stripe | 2 | No PIN entry capability |
| 05 | ICC Read |  |  |
| 80 | Magnetic stripe even  though it is ICC capable, fall back transaction |  |  |
| 81 | IPG (E-COM)  Transactions |  |  |

#### POS Condition Code, Field 25

The POS condition code is used to identify the condition under which the transaction takes place.

|  |  |
| --- | --- |
| Code | Meaning |
| 00 | Normal presentment |
| 01 | Suspected Fraud transaction |
| 03 | Merchant suspicious |
| 04 | ECR Interface |
| 05 | Customer present, Card not present |
| 06 | Pre-authorization |
| 08 | Mail and/or telephone order |
| 09 | SIRP transactions |
| 10 | Card holder activated terminal transaction |
| 71 | Card present mag stripe bad |

#### Acquirer Institution Code, Field 32

This code identifies the financial institution acting as the acquirer of this customer transaction. The acquirer is the member or system user that signed the merchant, installed the ATM or ADM, or dispensed cash

#### Track II data, Field 35

The Track II data field is present when valid track II is used to initiate the transaction. It contains the track II image excluding the start sentinel, end sentinel and LRC characters.

#### Retrieval Reference number, Field 37

The host assigns the RRN. The terminal stores the reference number and includes it on all advice transactions. If an advice receives a new RRN the terminal will replace the old RRN with the new value.

#### Authorization Identification Response, Field 38

Usually referred to as the “approval code.” Assigned by the authorization host when the transaction is approved.

#### Response Code

AWL host sends the response to the terminal to indicate the status of the transaction. A 00 response code indicates a host approval status. All other values are non-approval or error responses.

#### Terminal Identification Number, Field 41

Card Acceptor Terminal ID (DE 41) uniquely identifies a terminal at the card acceptor location. This data element is used for the terminal identification code associated with the terminal devices of acquiring institutions or merchant systems. Each terminal ID may be up to eight characters long and the terminal owner assigns it. It must be unique within the terminal owning organization.

#### Merchant Identification Number, Field 42

Card Acceptor ID Code (Field 42) identifies the card acceptor that defines the point of the transaction in both local and interchange environments.

Field 42 is used as a “merchant ID” to uniquely identify the merchant in the transaction request.

#### Card Acceptor Name and Location, Field 43

Field 43 contains the name and location of the card acceptor (such as merchant or ATM).

#### Transaction currency Code, Field 49

ISO code of the currency used in the transaction.

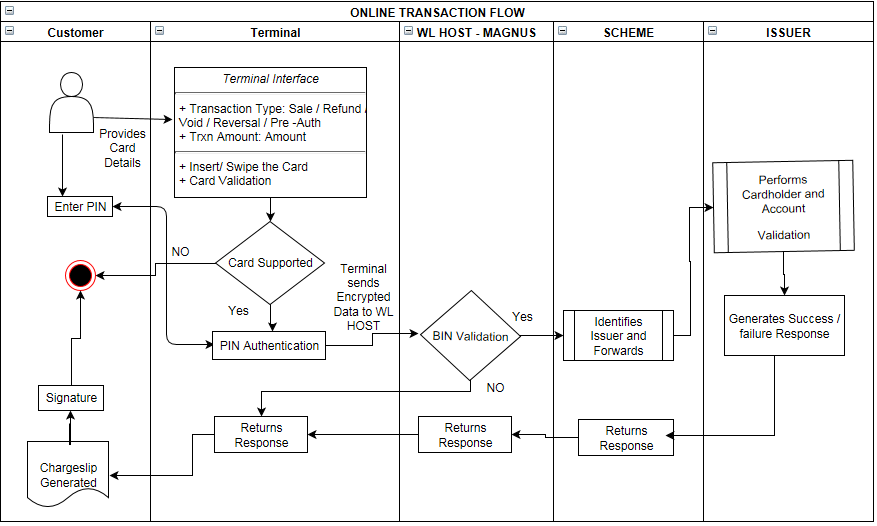
#### Personal Identification Number, Field 52

Encrypted PIN data

#### Amount Additional, Field 54

Request message contains the tip amount or fee amount. Response message will contain balance amount.

### Online Transaction Flow for Off-us Transactions



|  |  |  |  |
| --- | --- | --- | --- |
| UC-001: Online Transaction Flow for Off-usTransaction | | | |
| **Description** | | This use case describes the online Off-us transaction flow | |
| **Actors** | | Customer, Terminal, WL Host, Payment Scheme, Issuer | |
| **Pre-Condition** | | 1. Preregistered card for the customer/cardholder from the Issuing bank 2. Pre generated MID/TID created in the WL Insight system 3. BIN already configured for the respective bank in the WL system | |
| **Post-Condition** | | Transaction is successfully completed | |
| **Transaction Flow** | | | |
| **Step** | **System/User Action** | | |
|  | Customer approaches the Merchant for the Acceptance of the Card for the Payment. | | |
|  | After inputting all the information, Terminal will prompt for Card swipe / Insert / TAP.  Merchant will Insert / Swipe / Tap the card on the terminal and the respective card details shall be captured on the terminal. | | |
|  | After capturing the card details on the terminal, the terminal will check for the Card to be valid for acceptance. | | |
|  | For supported EMV Card, terminal will prompt for PIN.  After inputting the PIN, the POS terminal will initiate the transaction to the WL Host – Magnus after performing necessary local validations on terminal. | | |
|  | The terminal application will further route the transaction to Magnus (WL Switch)  Magnus will validate the respective transaction details and further route the transaction to Scheme (Visa/MasterCard/NPCI) | | |
|  | Scheme will further route the transaction to Issuer for authorization | | |
|  | Issuer will validate the Card holder details and provide the authorization response back to Scheme. | | |
|  | Scheme will further route the response back to WL switch Magnus. Magnus will further return the response back to terminal. | | |
|  | Post receiving response, POS terminal will display the transaction status and physical copy of chargeslip shall be printed by the Terminal for all successful transaction types viz, Purchase, Cashback, Refund, Void, and Pre-Auth. | | |
| **Business Rules** | | | |
|  | Terminal will prompt for Mandate Insert in case of EMV Card. | | |
|  | The PIN block and track 2 data encryption at the POS terminal shall be taken care at the Terminal Application level. | | |
|  | The authorization Data for the transaction from the POS terminal shall also be line encrypted to be sent to the Magnus (WL Switch). | | |
|  | In case of time out reversal, physical chargeslip shall be generated for the transaction | | |
|  | For Balance Inquiry transactions on Maestro Cards, terminal shall display the Balance and no chargeslip shall be printed. | | |
|  | The chargeslip shall be required to be signed by the customer in case the transaction is not PIN Authenticated. Else, the Chargeslip shall print “PIN Verified Ok, Signature not required. | | |
|  | The PAN Number shall be masked in all the copies of the chargeslip and Terminal Reports. | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | BIN is not configured or does not matches at the Host level | | Appropriate error message will be displayed with the reason code stating the failure of transaction |
|  | Bank Code is not configured in the | | Appropriate error message will be displayed with the reason code stating the failure of transaction |
|  | MID(s) is not configured or blocked at the Host level | | Appropriate error message will be displayed with the reason code stating the failure of transaction |
|  | Invalid Amount entered for a transaction | | Appropriate error message will be displayed with the reason code stating the failure of transaction |
|  | Incorrect PIN entered | | Appropriate error message will be displayed with the reason code stating the failure of transaction |
|  | Card is expired (If Expiry Date check is  enabled for the BIN range) | | Appropriate error message will be displayed with the reason code stating the failure of transaction |
|  | Transaction Limit exceeds the preset limit | | Appropriate error message will be displayed with the reason code stating the failure of transaction |

## Clearing Settlement and Chargeback Module - Cronus

Cronusmodule would be used for Clearing & Settlement and Chargeback management. This module functions as per the Payment Scheme guidelines i.e. by MasterCard/Visa and NPCI.

Key Features of Cronus:

* Generates Base II outgoing file for first presentment for MasterCard/Visa and RuPay.
* Processes Incoming files
* Extracts retrieval request and chargeback details from incoming file. WL will send a report on chargebacks to the bank.
* Generates re-presentment outgoing file on chargeback cases and send that to Schemes.
* Provision to process all exception transactions (Refund/Reversal/Fraud reporting, Fees, Funds)
* The JVs generated shall consist of the entries related to disputes as per the format in MIS / Reports.

### Base II Processing – Incoming

|  |  |  |  |
| --- | --- | --- | --- |
| UC-001: Base II Processing – Incoming File | | | |
| **Description** | | This use case describes about the Base II processing that happens in the Cronus module | |
| **Actors** | | FSD Team, Cronus | |
| **Pre-Condition** | | Processed batch from kalkulus stored at the specific location is already present | |
| **Post-Condition** | | Batch processing is completed for the particular file | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
| 1 | User logs into the Cronus module.  User selects the Data Upload🡪Transaction Processing option from the Cronus module to upload the processed batch from the Kalkulus. | |  |
| 2 | The file is uploaded from the *<<bank>>* input folder | |  |
| 3 | User selects the Submit button to process the file. | | The System processes the file and displays a “Process Summary” report on the screen. |
| **Business Rules** | | | |
| 1 | Only transaction files (.BTH files) can be uploaded for processing. Refer [Annexure R](#_Annexure_1) | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
| 1 | Invalid file is uploaded in the Cronus for processing | | Appropriate error message will be displayed on the screen stating the reason for failure |

### File Staging – Outgoing

|  |  |  |  |
| --- | --- | --- | --- |
| UC-002: File Staging – Outgoing File | | | |
| **Description** | | This use case describes about the file staging process that happens in the cronus | |
| **Actors** | | FSD Team, Cronus | |
| **Pre-Condition** | | Base II processing is already performed for the batch file | |
| **Post-Condition** | | Outgoing file is generated which is stored at specific location as per the schemes | |
| **Main Flow** | | | |
| **Step** | **User Action** | | **System Action** |
| 1 | User logs into the Cronus module | |  |
| 2 | **For Visa :**   1. In order to create an outgoing file, user selects the Base II 🡪 Outgoing 🡪 Submit 2. Once the user selects the submit button, the system shows process summary. | | The outgoing file is generated in the Output folder for the specific bank. |
| 3 | **For Master :**   1. In order to create an outgoing file, user selects the IPM 🡪Outgoing 🡪 Submit 2. Once the user selects the submit button, the system shows process summary | | The outgoing file is generated which is stored in the specific destination as per the user |
| 4 | **For Rupay :**   1. In order to create an outgoing file, user selects the Rupay 🡪Outgoing 🡪Submit 2. Once the user selects the submit button, the system shows process summary | | The outgoing file is generated which is stored in the specific destination as per the user |
| **Business Rules** | | | |
|  | XML file if generated for Rupay transactions. In case of Mastercard, IPM file is generated, (Refer [Annexure S](#_Annexure_1) and Annexure V) | | |
|  | For Visa, VO file (outgoing file) and ICTF file (For ONUS txns) are staged. (Refer Annexure V) | | |
|  | The BTHIN report is generated which contains the scheme wise transaction summary report of the Bank. (Refer [Annexure T](#_Annexure_1)) | | |
| **Exceptional Flow** | | | |
| **Sr. No.** | **Exception** | | **Error Message** |
|  | Invalid file is uploaded in the Cronus for processing | | Appropriate error message will be displayed on the screen stating the reason for failure |

### Chargeback process and Dispute management

Chargeback Processing shall be done by WL. A sample report that shall be shared with the Bank is attached in the [Annexure H](#_Annexure_1). Further the recoveries shall be done by the Bank Ops team for the respective merchants.

The document collection for Case to case basis chargeback handling and Merchant interactions shall be managed by BANK Ops team.

Dispute Management: For this Cronus module will be utilized. Detailed reference regarding the Dispute Resolution Management process is given in [Annexure I](#_Annexure_1)

## Reconciliation Process

* WL will prepare outgoing file which will detail out INR transactions and send it to Payment Scheme.
* WL will reconcile the merchant payout with Outgoing file before staging.
* Payment Scheme will credit the amount in the Bank’s account in INR/USD as agreed upon by the Payment Scheme and bank.
* Funds will be received through the Incoming file from MasterCard/Visa and NPCI for the transactions staged.
* Rupay SMS and Maestro reconciliation process shall be done by WL through two way recon process. Recon alert needs to be built from ISO BTH to Processed BTH.

Currently exception report is generated for Maestro Report as per attached format in [Annexure M](#_Annexure_1).

### Rupay Recon Process:

During reconciliation, WL will check whether WL has received credit from associations for the payments made to merchants.

WL will match the PAYOUTS made to merchant with the SETTLEMENT Received. The files required are SETTLEMENT RAW DATA Files(831/021/041) from RGCS & Merchant Payment file from Kalkulas.

The Settlement files received from NPCI comes in an encrypted format which is decrypted at the WL end. The decrypted settlement files are merged date-wise at WL and this file is matched with the CBS/GL entries. A summary is prepared after the transaction matching of these entries.

After the Data/Summary matching, the Merchant Payment file received form the Kalkulus is matched with the decrypted Settlement File and a summary of the data is generated. The Rupay Recon file will contain a summary of the following:

* Surcharge – dms/dfs
* Tip Transactions-BOTH
* Failed txns (By npci) – Timing
* Wrong/Missing GL postings by bank
* Chargeback/Refunds
* **Debits in a/c - Claimed by ME but not settled by NPCI**
* **Credits in a/c – Settled by NPCI but not claimed by ME**

### Maestro Reconciliation Process:

During Reconciliation, the Merchant payment file generated from the Kalkulus and the Incoming file (TT464) from the Maestro scheme is uploaded into the Maestro Recon Module. The output file generated is a log file – log 1 and log 2. Log 1 file contains the matching records while Log 2 contains the exceptions (Chargeback, reversals)

Following are the reports that are generated:

* EXCEPTION-PENDING-TXNS-00045-010816
* MECLAIM-NOTSETL-MCI-00045-010816 - Meclaim
* SETTLEDMCI-NOTCLAIMED-ME-00045-010816 - Settled mci
* Log 1
* Log 2
* GL from Bank

These reports are to be matched with GL accounting entries. WL will take the last running balance as closing balance GL balance then match (VLookup) the exception file with settled mci & Meclaim File. The sum of unmatched (NA) transactions derived from settled mci & Meclaim file are taken as items in Recon Working sheet. The unmatched Meclaim amount is lessen from the GL balance of that particular day and the unmatched settled mci amount is added to the GL balance respectively. The exceptions found are to be lessen from the GL balance.

* 1. Chargeback entries in GL
  2. Additional amount of any TID
  3. Unidentified entries

## Risk Monitoring

* WL team will monitor the merchant transactions alerts generated by OLW (Online watcher) as per preset rules and share the actions with the Bank as per timelines agreed and also hold the payments wherever warranted and inform to the bank. Once the documents received with the concurrence of the Bank, WL will release the payments.
* Outbound calling wherever warranted for suspicious transactions during monitoring will be done by WLI Risk team.
* For all the cases where the merchant funds have been put on hold by WLI during monitoring, a file will be shared with the Bank. The Bank will arrange to intimate the respective merchants and arrange for supporting documents.
  + Payment Holdover/Release module shall be managed in Kalkulus, please refer the sample reports in [Annexure E](#_Annexure_1).
  + [Annexure K](#_Annexure_1) describes the process for Risk Monitoring activity and Holdover/release of Merchant payments
* **Bank shall be enabled for WL FRM Tool.**
* The rules mentioned in [Annexure J](#_Annexure_1) are the indicative rules of Acquiring will be shared with Bank by WL.
* The Bank will decide on the list of FRM Rules that they would opt for. Flexibility available in WL systems for setting of rules. The transaction monitoring will be done on near-real time basis

## Help Desk / Merchant Call Center

Help desk number will be printed on the terminal sticker and user manuals will be provided to merchant. Bank to provide (if required) VISA / MasterCard / Rupay logo stickers to FSD team and it will be handed over to merchant.

Inbound call will be handled by Helpdesk team and the following activities are undertaken:

* Handling all Merchant Service Issues within agreed TATS
* Logging all Merchant Calls on Insight Complaint Management System
* Audit report of all complaints with complete trail from date of complaint, status, and date of resolution
* Call Centre team will do follow-ups with Merchants for unsettled transactions.
* Voice Authorization
* Pre Auth Cancellation: As per the current mandate, after 30 days the transaction gets deleted at the POS and OTBL is being restored at the issuer. In case of cancellation before 30 days, the current manual process as mandated by Visa and MasterCard will be applicable.

# Certifications

Following certifications would be required for EMV Compliance over various Schemes

* ADVT/EMV terminal Certification
* Master Card MTIP terminal Certification
* Visa and Master Card Host Certification
* RUPAY terminal and Host Certification
* NFC Certification – PayPass and Paywave with MC and Visa respectively

EMV L1 and L2 certification would be done by OEM along with Schemes.

In case of MasterCard and Visa, base1 and base 2 certification required. In case of NPCI, File based and host certification required.

Host Certification with Schemes shall be supported by WL as advised by the respective Scheme Visa / MasterCard / Rupay as and when taken up by the Bank.

# Billing

Billing Invoice for Bank shall have the below logic as agreed with the Bank.

* Per Terminal Per Month Service Fee (number of terminals \* per terminal charges). This will be based on Active Terminals available in Insight.
* The Billing module shall be detailed in discussion with the WL Finance Team
* One time set up Fee Applicable for the Bank

# Non- Functional Requirements

* 1. Performance

1. All mandatory field validation should also be done at client end to avoid server hits.
2. EMI File should be processed in maximum of 15 mints (For 10,000 records)
   1. Audit Trails

The following events will be logged for audit purpose.

1. EMI transaction file processing log having success and failure status, date and time of receipt and process along with the user name should be stored in the system.
2. Records covering match and un-match EMI transactions details should be stored in the system.
3. Logs must be created for the SMS sent and received (as per Annexure x)
4. When converting a transaction to EMI transaction, original transaction must be stored in the system.
   1. Access Controls

WL Operation user will have access to receive EMI transaction file from bank and to process it in WL systems rest of the access controls will remain as is.

* 1. Security Controls

Card Number should be stored in database using TDE.

* 1. Data Retention Period

EMI data file processing log will be purged from the system post 1 year.

EMI transactions will be purged from the system post 5 years.

# Annexure

|  |  |  |
| --- | --- | --- |
| **Annexure** | **Reference Document Name** | **Document** |
|  | Sample Bulk Onboarding File and Mandatory fields |  |
|  | Sample Bulk Onborading Log Formats |  |
|  | Sample Insight Screen Shots and Insight Sample Reports |  |
|  | Sample EOD Reports |  |
|  | Sample Payment Hold/ Release Report |  |
|  | Sample TTUM File |  |
|  | NEFT file format | Bank to confirm. |
|  | Cr/Dr Host Message Specifications File |  |
|  | Sample Chargeback Report |  |
|  | Dispute Resolution Management Process Note |  |
|  | FRM Acquiring Rules |  |
|  | Process note for Risk Monitoring of Merchant activity and Holdover/release of Merchant payments |  |
|  | Sample Maestro Reports and ISO BTH Recon Report ( for WL Ops Team) |  |
|  | Sample Journal Vouchers |  |
|  | Sample Risk Reports |  |
|  | NFC Acquiring Process |  |
|  | Merchant Payment Advice |  |
|  | Differential MSF Note |  |
|  |  |  |