**ÆON Credit Service Systems (Philippines) Inc.**

**Credit Card Systems Cambodia**

**Requirements Definition**

**Functional Requirements**

**Specification**

**Version 0.03**

**01/16/2014**

**Revision History**

| Revision History | | | | |
| --- | --- | --- | --- | --- |
| Version No. | Date | \*A/M/D | Details of Change | Prepared By |
| 0.01 | 06/25/2013 | A | Initial Draft | J. Cruz |
| 0.02 | 01/14/2014 | M | Modification according to review / correction points | E. Lanorio/J. Alabat / K. Labustro / F. Jaurigue |
| 0.03 | 01/16/2014 | M | Modification according to review / correction points by QAS | J.Cruz |

**Note: \*A- Added M-Modified D-Deleted**

This document has been reviewed as the official **ACSKH Credit Card Systems – Functional Requirements Specifications.** Following review of this document, changes will be checked by all relevant stakeholders such as Team Leads and Project Managers.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Review History** | | | | |
| **Date** | **Version No.** | **Reviewer’s Name** | **Project Role** | **Remarks** |
| 12/04/2014 | 0.01 | J. Cruz | Project Coordinator | For modification of all teams to include all systems’ details. |
| 01/15/2014 | 0.02 | J. Cruz | Project Coordinator | For QAS Submission. |

**Table of Contents**

1. INTRODUCTION 1

1.1 Purpose 1

1.2 In Scope Functionalities 1

1.3 Out Of Scope Functionalities 3

1.4 Definitions, Acronyms, and Abbreviations 4

1.5 References 15

2. SOLUTIONS 17

2.1 Credit Card System Background 17

2.2 Proposed System Configuration 21

2.3 Proposed Network Configuration 22

2.4 Functionalities 25

2.4.1 NEW FEP Functions 27

2.4.2 Monitoring System Functions 37

2.4.3 HOST Functions 47

2.4.4 AFIS Functions 51

3. FUNCTIONAL REQUIREMENTS 53

3.1 FR001 Application Process 54

3.2 FR002 Embossing Process 60

3.3 FR003 Card Activation Process 62

3.4 FR004 Account Management 65

3.5 FR005 PIN Generation Process 73

3.6 FR006 Cards Transactions 75

3.7 FR007 Settlement Process 89

3.8 FR008 Daily Sales Closing Process 93

3.9 FR009 Statement Process 95

3.10 FR010 End of Month Process 98

3.11 FR011 Payment 101

3.12 FR012 Collection Process 103

4. NON-FUNCTIONAL REQUIREMENTS 105

4.1 Certification / Central Bank Audit Requirements 105

4.2 Reliability 105

4.3 Performance 107

4.4 Security 107

4.5 System Operations and Maintenance 108

4.6 Scalability 108

5. Assumptions and Dependencies 109

6. Information and Approval Section 110

# INTRODUCTION

* 1. Purpose

This document defines the business, operational and high-level functional requirements of AEON MICROFINANCE (CAMBODIA) PRIVATE COMPANY LTD, or known as ACSKH for the Credit Card System Project. It shall be used as the basis for the following activities:

* Creation/Customization of solution designs for ACSKH Host Systems and ACSKH AEON Financial Information System (AFIS).
* Customization of solution designs for the ACSKH New Front End Processing System (New FEP).
* Development of test plans, test scripts, and test cases.
* Scope and Coverage of the Project Completion.
  1. In Scope Functionalities

For ACSKH Common Credit Card Systems, the following transactions will be in scope for the first Phase of the Project (On-Us Transactions not in scope for Phase-1):

**Legend:**

|  |  |
| --- | --- |
| **S**  (Supported) | Transactions can be addressed / processed in the ACSKH Credit Card System. NEW FEP receives this transaction, sends to HOST for approval or decline |
| **NS**  (Not Supported) | Transactions will not be processed in the ACSKH Credit Card System. Transactions that can be supported but due to ConOps specs or services confirmed with VISA and MasterCard, NEW FEP implemented not to support this and will not send to HOST or will not receive this type of transactions from VISA/MasterCard by default. |
| **NA**  (Not Applicable) | Scenario is not possible. |
| **CNP**  (Card Not Present) | Transactions wherein the card/cardholder is not physically present during the transaction.   * E-commerce (e.g. Internet Transactions from other merchants like Amazon) * Mail Order / Telephone Order (MOTO) * Recurring Payments |

Based on Figure 1.2 Credit Card Transaction Matrix, the following type of Card Transactions will be supported:

1. EMV/IC Chip
2. Magnetic Stripe
3. Manual Card Entry / MOTO/E-Commerce (EC)
4. Fall-back Transaction (EMV to Magnetic Stripe)

|  | **Transaction** | | **VISA** | | | **MasterCard** | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **EDC** | **ATM** | **CNP** | | **EDC** | **ATM** | **CNP** |
| 1 | Cash Advance | EMV/IC | S | S | NA | | S | S | NA |
| Mag Stripe | S | S | NA | | S | S | NA |
| Manual | NS | NA | NA | | NS | NA | NA |
| Sales | EMV/IC | S | NA | NA | | S | NA | NA |
| Mag Stripe | S | NA | NS | | S | NA | NS |
| Manual | S | NA | S | | S | NA | S |
| Balance Inquiry | EMV/IC | NS | S | NS | | NS | S | NS |
| Mag Stripe | NS | S | NS | | NS | S | NS |
| Manual | NS | NS | NS | | NS | NS | NS |
| 2 | PIN Change | EMV/IC | NS | NS | NS | | NS | NS | NS |
| Mag Stripe | NS | NS | NS | | NS | NS | NS |
| Manual | NS | NS | NS | | NS | NS | NS |
| Card Activation | EMV/IC | NS | NS | NS | | NS | NS | NS |
| Mag Stripe | NS | NS | NS | | NS | NS | NS |
| Manual | NA | NA | NA | | NA | NA | NA |
| 3 | Reversal/Reversal Advice | EMV/IC | S | S | S | | S | S | S |
| Mag Stripe | S | S | S | | S | S | S |
| Manual | S | S | S | | S | S | S |
| Authorization Advice | EMV/IC | S | S | S | | S | S | S |
| Mag Stripe | S | S | S | | S | S | S |
| Manual | S | S | S | | S | S | S |

**Figure 1.2 Credit Card Transaction Matrix**

* 1. Out Of Scope Functionalities

The following functionalities will be considered out of the scope for the first phase of the ACSKH Credit Card Systems Project:

* Fraud Monitoring and Velocity Checking Functionalities (ACEPlus)
* Actual Physical Card Creation**\***
* PIN Printing Functionalities**\*\***
* Card Mailer other than the Welcome Letter
* Collection Reminder Letter
* On-Us Transaction Functionalities
* ATM connection
* EDC connection
* Online Web

**Note:** **\*** ACSKH has mentioned that this will be done in-house.

**\*\*** ACSKH has to confirm as to how they would implement the printing of PIN Letter

* 1. Definitions, Acronyms, and Abbreviations

| **Term/Acronym** | **Meaning / Definition** |
| --- | --- |
| ACEPlus | Alarm for Credit Card Effectuation (ACE) or ACEPlus  A fraud detection system. It provides card transaction monitoring, alerts, and automatic detection of suspicious transactions. |
| Acquirer | Also referred to as “acquiring bank” or “acquiring financial institution.” Entity that initiates and maintains relationships with merchants for the acceptance of payment cards. |
| ACSKH | AEON Microfinance (Cambodia) Co., Ltd.  Client / Company requesting for the Credit Card System to be implemented in Cambodia. |
| ACSS | AEON Credit Service Systems (Philippines) Inc.  Company Responsible for providing the Credit Card System for ACSKH. |
| AFIS | AEON Financial Information System.  A system which captures the process of applying for a loan to buy goods or product. Generally, AFIS captures the steps from loan application up to management of credits until the loan is fully paid off. |
| Agency Code | Also pertains to Merchant Code.  E.g. 0742 Veterinary / 3022 Philippine Airlines |
| ARPC | Application Response Cryptogram.  A cryptogram generated by the issuer in response to an Authorization Request Cryptogram. |
| ARQC | Authorization Request Cryptogram.  An Application Cryptogram generated by the card when requesting online authorization. |
| ATM | Automated Teller Machine.  The new overseas FEP system receives the message from the ATM and responds with the processing result. (ATM Status Management, Processing Fee Collection, ATM Control, security management, ATM transaction management, etc.) |
| Authentication | The provision of assurance of the claimed identity of an entity or of data origin.  Authentication is the process of verifying identity of an individual, device, or process. Authentication typically occurs through the use of one or more authentication factors such as:   * Something you know, such as a password or passphrase * Something you have, such as a token device or smart card * Something you are, such as a biometric |
| Authorization | Granting of access or other rights to a user, program, or process.   * For a network, authorization defines what an individual or program can do after successful authentication. * For the purposes of a payment card transaction, authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor. |
| Backup | Duplicate copy of data made for archiving purposes or for protecting against damage or loss. |
| BIN | Bank Identification Number.  The number the brand assigns the member (card company). The first 6 characters of the card number |
| Business Code | In AS400 programs, this refers to the actual card brand.  (e.g. VS – VISA ; MC – MasterCard) |
| CA | Cash Advance  Petty cash loans for credit card members. |
| CAD | Credit Assessment Department.  Department responsible for processing of Applications. |
| Card Verification  Code or Value | Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features.   1. Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand:    1. CAV – Card Authentication Value (JCB payment cards)    2. CVC – Card Validation Code (MasterCard payment cards)    3. CVV – Card Verification Value (Visa and Discover payment cards)    4. CSC – Card Security Code (American Express) 2. For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit un-embossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following list provides the terms for each card brand:    1. CID – Card Identification Number (American Express and Discover payment cards)    2. CAV2 – Card Authentication Value 2 (JCB payment cards)    3. CVC2 – Card Validation Code 2 (MasterCard payment cards)    4. CVV2 – Card Verification Value 2 (Visa payment cards) |
| Cardholder | Cardholder Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card. |
| CB | Card Brand  May pertain to VISA / MasterCard/ JCB/ CUP, etc. |
| CCS | Credit Card System.  System provided by ACSS composing of HOST, AFIS and NEW FEP Systems. |
| CIF | Customer Demographic and Financial Information. |
| Closing Date | Pertains to system’s (computer) date upon running the AS400 Process. |
| CNP | (Card Not Present) transactions. A card not present transaction is a payment card transaction made where the cardholder is not physically present with the card at the time that the payment is made. CNP Transactions include mail order, telephone order, electronic commerce, partial authorization, recurring payment, installment payment, or contactless. |
| ConOps | Concept of Operations (ConOps) is a document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system. |
| CP | Credit Purchase  Sales transaction done thru EDC/POS Terminal |
| Cryptogram | Result of a cryptographic operation. A numeric value that is the result of data elements entered into an algorithm and then encrypted; commonly used to validate data integrity. |
| CSPS | Correspondence Series Printing System.  CSPS has no direct connection with HOST or NEW FEP, but can generate reports having flat files as inputs. |
| Currency Conversion Rate | Is the current Card brand defined currency exchange rate. This will be provided to Issuers as a part of their services. |
| CVK | A Card Verification Key (CVK)  Similar to a PIN Verification Key, but for Card information instead of a PIN. |
| CVV | Card Verification Code or Value.  Security code used as a fraud countermeasure for VISA card. Encoded in the magnetic stripe. There is also a CVV2 displayed on the back of the card. |
| Database | Structured format for organizing and maintaining easily retrievable information.  Simple database examples are tables and spreadsheets. |
| DES | Data Encryption Standard.  A cryptographic algorithm in which two users share the same secret key.  In cryptography, a key is a value that determines the output of an encryption algorithm when transforming plain text to its encrypted value. The length of the key generally determines how difficult it will be to decrypt the encrypted value in a given message. |
| DR | Disaster Recovery.  Process, policies and procedures that are related to preparing for recovery or continuation of technology infrastructure which are vital to an organization after a natural or human-induced disaster. |
| EAS | Extended Access Server.  Access device that resides at endpoint or within Visa network. BASE II data are generally transmitted or received through an EAS. |
| EDC | Electronic Data Capture.  A device (usually a point-of-sale terminal) that is cable of reading and processing data from magnetic stripe and chip cards. |
| Embossing | Characters raised in relief from the front surface of a card. |
| EMV | Europay, MasterCard and VISA.  A global standard for inter-operation of integrated circuit cards (IC cards or "chip cards") and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions. |
| EMVCo | EMVCo, owned by American Express, JCB, MasterCard, UnionPay and VISA, manages, maintains and enhances the EMV®1 Integrated Circuit Card Specifications to ensure global interoperability of chip-based payment cards with acceptance devices including point of sale terminals and ATMs. |
| Encryption | Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure. |
| Fallback Transaction | The term used for the scenario when an EMV chip card transaction is initiated via its magnetic stripe at an EMV chip terminal. This may be the result of an inoperative chip on the card or a malfunction of the terminal chip reader. |
| NEW FEP | New Front End Processing.  A product owned by ACSS and is an automated system communicating with the Card Brand Network using ISO 8583 message format for credit card transactions. It acts as the bridge between the network and Host, ACEPlus, HSM, AEON POS and ATM terminals and aims to complete the authorization of transactions. |
| FTP | File Transfer Protocol.  Network protocol used to transfer data from one computer to another through a public network such as the Internet. FTP is widely viewed as an insecure protocol because passwords and file contents are sent unprotected and in clear text. FTP can be implemented securely via SSH or other technology. |
| Handling Charge | Refers to charges on CA transactions that will be defined by the client. |
| HOST or AS400 | Used interchangeably to refer to the system that authorizes transactions. The Host manages database, maintains customer accounts, processes settlement, and supports routine credit card operation and maintenance activities. |
| HSM | Host Security Module.  A hardware-based security appliance that generates and validates Card Verification Values (CVV) and PIN. |
| ICC | Integrated Circuit(s) Card, also referred to as “chip card” or “Smart card” is a type of payment card that has integrated circuits embedded within the card. The integrated circuit also referred to as the “chip,” contains payment card data including but not limited to data equivalent to the magnetic-stripe data. |
| iCVV | iCVV – Card Verification Value for Integrated Circuit Cards. |
| ISO | An independent sales organization sells credit card services to merchants on behalf of an acquiring bank. The ISO is a separate organization, and is typically not affiliated with a single acquiring bank. |
| ISS | Issuing  Credit Card Transactions using AEON Card in Non AEON Terminal. |
| Issuer | Entity that issues payment cards or performs, facilitates, or supports issuing services including but not limited to issuing banks and issuing processors.  Also referred to as “issuing bank” or “issuing financial institution.” |
| ITR | Income Tax Return  A document giving the tax collector information about the taxpayer's tax liability. |
| LCP | Line Control Process  New FEP component for line status checking of External Network Connection |
| Mag Stripe | Magnetic Stripe - The stripe containing magnetically encoded information |
| Magnetic Stripe Data | Magnetic-Stripe Data Also referred to as “track data” refers to the data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. It can be the magnetic stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe. |
| MC | MasterCard  An American multinational financial services corporation headquartered in the MasterCard International Global Headquarters, Purchase, New York, United States. |
| MCP | Message Control Processing  Used by NEW FEP for message parsing and validation |
| MDK | Master Derivation Key  In the context of EMV, the MDK is the top symmetric key in a hierarchy where the MDK is generated, owned and store by the card issuer in a secure device such as an HSM at its host. |
| MIP | MasterCard interface processor (MIP)  A front-end communications processor placed on-site at a MasterCard customer’s facility or at a processor or hub site. The MIP provides access to the MasterCard Worldwide Network.  MIPs provide access to all MasterCard electronic funds transfer (EFT) products and to a wide variety of other EFT services via MasterCard gateways. MIP software supports issuing and acquiring functions, including routing MasterCard transactions to issuers, acquirers, and Stand-In System processing and switching non-MasterCard transactions to appropriate destinations via the gateways. |
| MSP | Member Service Providers.  Institutions providing Credit/Debit card services affiliated to the Card Brand Network |
| On-Us Transactions | Card transactions that are accepted from terminals of merchants who have card service agreements with ACSKH. |
| PAN | Primary Account Number  Also referred to as “account number.” It is a unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder’s account. |
| PCI DSS | Payment Card Industry Data Security Standard  A proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. |
| PIN | Personal Identification Number.  A secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder’s signature. PIN is required for Cash Advance Transactions |
| PIN Block | A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length, and may contain subset of the PAN. |
| PIN Offset | The encrypted PIN value. The encrypted PIN value is used to verify the authenticity of the PIN by matching it against the value from NEW FEP and the HSM. |
| POS | Point of Sale  Hardware and/or software used to process payment card transactions at merchant locations. |
| Response | A message returned by the ICC to the terminal after the processing of a command message received by the ICC. |
| Router | Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways. |
| Sales Type | Refers to Cash Advance Transactions types such as Counter Loan, Cash Dispenser, and other fees. |
| Server | Computer that provides a service to other computers, such as processing communications, file storage, or accessing a printing facility. Servers include, but are not limited to web, database, application, authentication, DNS, mail, proxy, and NTP. |
| Service Provider | Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded. |
| Short Payment  (Small Billing) | Refers to the account state where after allocating the payment to the Minimum billing, there is a small billing left. |
| SMS | Short Message Service (AFIS)  Is used to send text messages to mobile phones  Single Messaging Service (VISA/FEP)  VISA Network Responsible for processing ATM Acquired Transactions |
| STIP | Stand-In Processing  Card Brand process of authorizing transaction if issuer is not available |
| TCP | Transmission Control Protocol.  Basic communication language or protocol of the Internet. |
| Terminal | The device used in conjunction with the ICC at the point of transaction to perform a financial transaction. The terminal incorporates the interface device and may also include other components and interfaces such as host communications. |
| TPIN | Telephone Personal Identification Number.  Commonly used for Mobile Authentication Process. |
| Transaction | An action taken by a terminal at the user‘s request. For a POS terminal, a transaction might be payment for goods, etc. A transaction selects among one or more applications as part of its processing flow. |
| VROL | VISA Resolve Online  A web-based application that supports customer service representatives and back-office analysts responsible for managing the dispute cycle for both BASE II and SMS, request for copies, fraud reporting and exception file management. In addition it is a mandated service used to exchange electronic dispute documentation and information. |
| VS | VISA  An American multinational financial services corporation headquartered in Foster City, California, United States. It facilitates electronic funds transfers throughout the world, most commonly through Visa-branded credit cards and debit cards. |

* 1. References

| **Document** | **Description** | **Version** | **Issue Date** |
| --- | --- | --- | --- |
| 05\_V.I.P.\_System\_BASE\_I\_Processing\_Specifications\_0847 | VISA Card Brand Manual that describes the processing requirements and options for the BASE-I System component of the VISA Net Integrated Payment (V.I.P.) System. It provides an overview of BASE-I and comprehensive information about BASE I message processing, including:   * Message types. * Message flows for authorization and non-authorization messages. * Message editing. * Message routing. * Authorization limits. * Stand-in processing (STIP). * Reversals and advices.   This manual also describes BASE-I user responsibilities and processing options and contains general information about the Cardholder Database and the Merchant Central File. These databases contain member-supplied data that BASE-I uses to process transactions as members specify. | N/A | Dec. 2012 |
| 06\_V.I.P.\_System\_BASE\_I\_Technical\_Specifications\_Vol\_1\_0844A\_DEC2012 | VISA Card Brand Technical Specifications Manual containing:   * Message Matching * Message Structure * Header Fields * Data Field Descriptions | N/A | Dec. 2012 |
| 07\_V.I.P.\_System\_BASE\_I\_Technical\_Specifications\_Vol\_2\_0844B | VISA Card Brand Technical Specifications Manual containing:   * This chapter contains the BASE I message charts. * Reject Codes * File Maintenance Error Codes * GMT Conversion * Country and Currency Codes * CRS Return Reason Codes * Batch File Maintenance * Electronic Reporting * VSDC Fields—Additional Information | N/A | Dec. 2012 |
| Customer Interface Specification | Contains the MasterCard implementation of the ISO 8583–1987 international message standard for processing authorization information using the MasterCard Dual Message System, Authorization Platform. It provides MasterCard customers with information necessary for development of an application-level online software interface between customer processor systems (CPSs) and the MasterCard Dual Message System. | N/A | May 2013 |
| Authorization Manual | Manual for the MasterCard Authorization Platform – an international message processing system that transmits authorization validation data among issuers, acquirers, and points of interaction.  The Authorization Platform refers to both hardware (the physical communications lines of the MasterCard Worldwide Network and MasterCard interface processors [MIPs]) and software (the MasterCard Network authorization application). | N/A | April 2013 |
| VISA Chip Terms Explained | A Guide to Smart Card Terminology | N/A | 2002 |
| EMV v4.2 Book 1 ICC to Terminal Interface CR05 | EMV Integrated Circuit Card Specifications for Payment Systems | 4.2 | 2008 |
| pci\_glossary\_v20 | Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS) Glossary of Terms, Abbreviations, and Acronyms | 2.0 | Oct. 2010 |
| AS400 Systems Operators and Users’ Manual | Manual for AS400 Screen / reports functions. | 1.0 | Jan. 2014 |

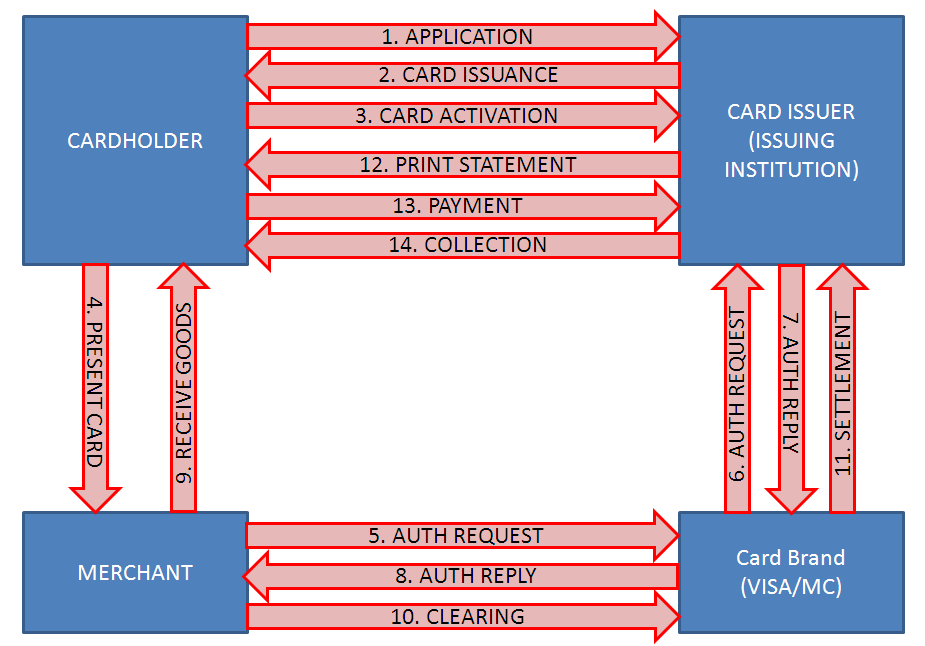
# SOLUTIONS

* 1. Credit Card System Background

**2.1.1 Credit Card Transaction Flow – Key Players**

1. **Cardholder**  
   A cardholder is a customer who owns a credit/debit card issued by legitimate Card Issuing Company. The customer then presents his valid card to merchants as payment for goods and/or services.
2. **Merchant**  
   A Merchant is a / or business entity that accepts credit/debit card for the goods and/or services it is offering. A Merchant needs to have an account with an Acquiring bank to be able to accept credit/debit card payment.
3. **Issuing Institution (Cardholder Bank)**

The issuing institution is also a member of the card associations (VISA and MasterCard). They are the company who are financing the purchases of the Cardholder and the one who issued the credit/debit cards to Cardholder. Issuing institutions settles all the purchases of their cardholder with acquiring institutions via the Card Brand (VISA/MasterCard). Cardholder’s will settle their payment to their respective Issuing institution under the terms of their credit card agreement.

 **Note: For this project, ACSKH is referred to as the Issuing Institution.**

**Figure 2.1.1 Credit Card Transaction Flow**

1. **Card Brand (VISA and MasterCard)**

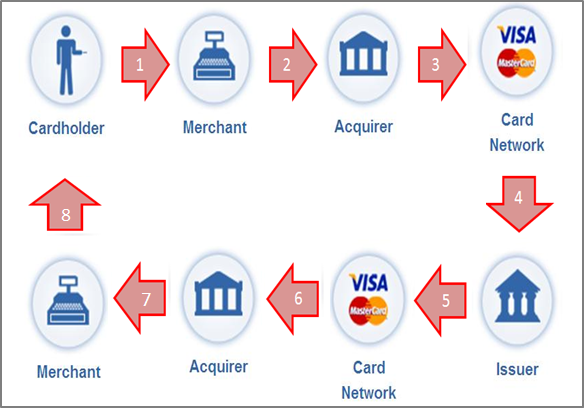
VISA and MasterCard act as custodian and clearing house for their respective card brand. They also function as the governing body of a community of financial institutions, ISOs and MSPs that work together in association to support credit card processing and electronic payments**.**

1. **Acquiring Institution (Merchant Bank)**

The Acquiring is a registered member of the card associations (VISA and MasterCard). An acquiring institution is often referred to as a merchant bank because they contract with merchants to create and maintain accounts that allow the business to accept credit cards. Acquiring institutions provide merchants with equipment and software to accept cards, promotional materials, customer service and other necessary aspects involved in card acceptance. The acquiring institution also deposits funds from credit card sales into a merchant’s account.

**Note**: Not yet included for ACSKH Credit Card System Implementation.

**2.1.2 Credit Card Authorization Flow**

**Figure 2.1.2 Credit Card Authorization Flow**

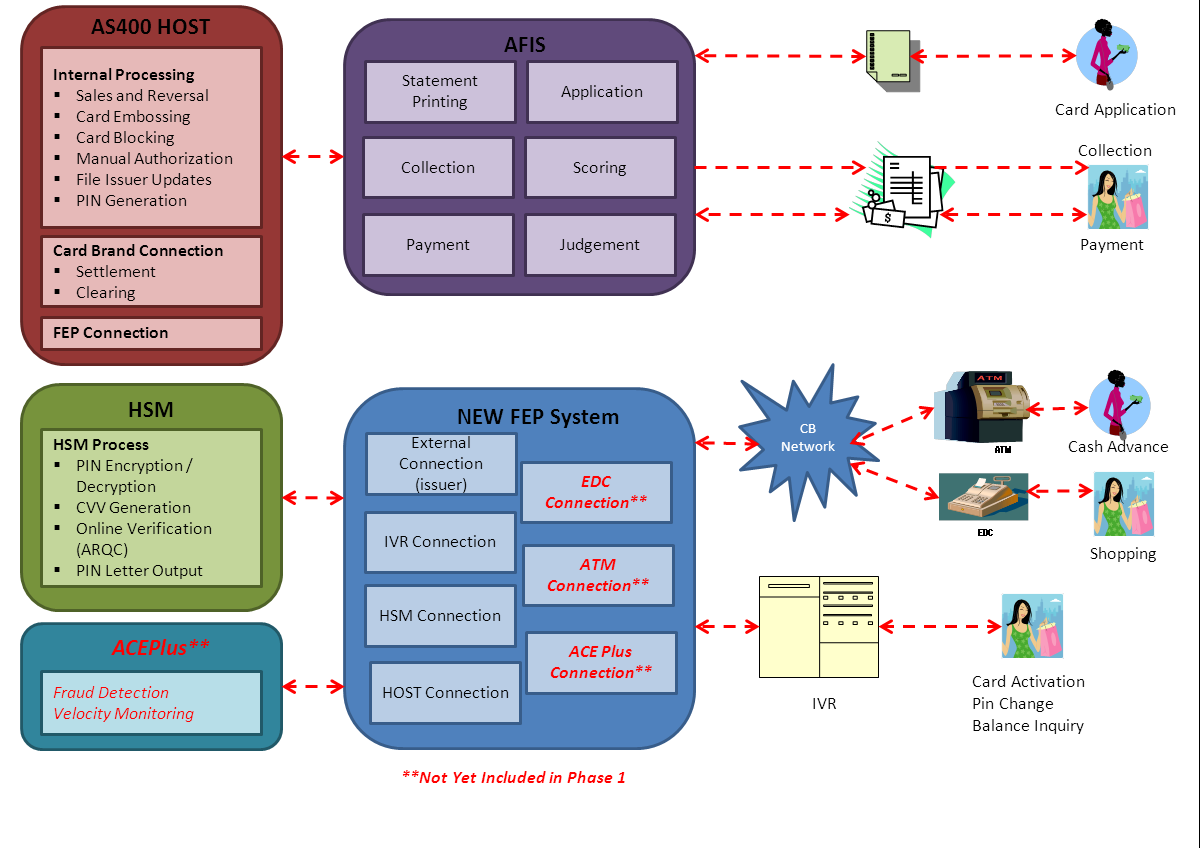
1. A Credit Card holder begins a transaction by presenting his/her card to a merchant as payment for goods and/or services.
2. The merchant uses their credit card machine (e.g. EDC /POS), software or gateway to transmit the cardholder’s information and details of the transaction to their acquiring bank, of the bank’s processor.
3. The acquiring institution (or its processor) captures the transaction information and routes it to through the appropriate card network to the cardholder’s issuing institution.
4. Transactions are routed to specific Card Brand Networks. The transaction need to be approved or declined by the Issuing Institution.
5. The credit card issuer receives the transaction information from the acquiring institution (or its processor) thru MasterCard/VISA and responds by approving or declining the transaction after checking to ensure, among other things, that the transaction information is valid, the cardholder has sufficient balance to make the purchase and that the account is in good standing.
6. The Card issuer sends a response code back through the appropriate network.
7. The acquiring bank (or its processor) will then receive the response code allowing or declining the request.
8. The response code reaches the merchant’s terminal, software or gateway and is stored in a batch file awaiting settlement.

**2.1.3 Credit Card Clearing and Settlement**

**Figure 2.1.3 Credit Card Authorization Flow**

1. A Merchant begins the settlement process by sending their batch of approved authorizations to their acquiring institution. Authorization batches are typically sent at the closing of each business day.
2. The acquiring institution reconciles and transmits the batch of authorizations through interchange via the appropriate card brand network.
3. The Card Brand network debit the issuing bank’s account and credits the acquiring institution account for the net amount of the authorizations which is gross receipts less interchange and network fees.
4. The card issuing institution essentially pays the acquiring institution for its cardholder’s purchases. The card holder is responsible for repaying his/her issuing institution for the purchase and any accrued interest and fees associated with the card agreement.

* 1. Proposed System Configuration

**Figure 2.2 Credit Card System Configuration**

The proposed solution and scope for this project will only cover the capacity for ACSKH to become an Issuing Institution for ACSKH and to quickly enter into the Cambodia Credit Card market. This will cover the Issuing businesses for both VISA and MasterCard Card brands.

The following functionalities and capabilities are proposed to be excluded in this project:

* EDC Connection
* ATM Connection
* Fraud Monitoring and related capabilities
* Online Web capabilities

* 1. Proposed Network Configuration

Figures 2.3-A Production Network Configuration Diagram and Figures 2.3-B DR Network Configuration Diagram illustrate a typical network infrastructure for an AEON Credit Card System implementation.

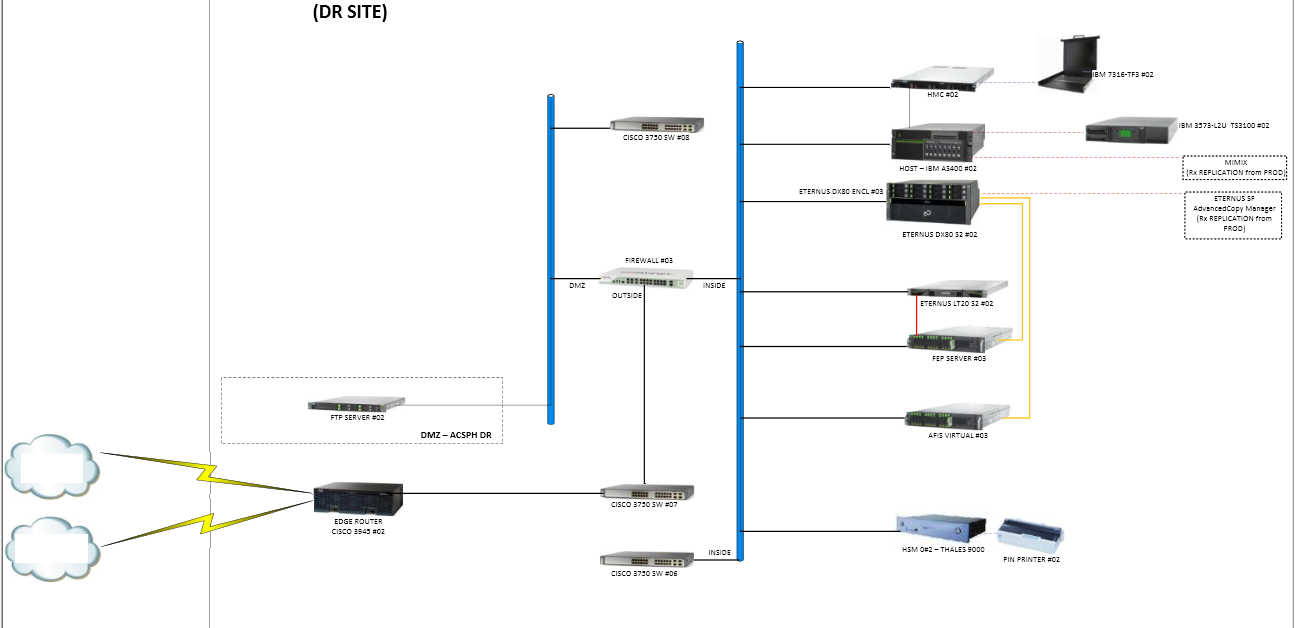
A full scale infrastructure implementation that includes both hardware and software components’ redundancy and automatic fail-over in case of system failure.

A Disaster Recovery Center is also necessary for guaranteed minimum downtime in case of unforeseen events that may happen on the production site.

For ACSKH implementation, a simplified infrastructure which **does not include automatic fail-over and hot standby** will be applied. A warm standby will be available at the Disaster Recovery Center in case of unrecoverable failure.



**Figure 2.3-A Production Network Configuration Diagram**



**Figure 2.3-B DR Network Configuration Diagram**

* 1. Functionalities

The ACSKH Credit Card Systems will include the following functionalities:

1. **AFIS**

* Application Scanning and Input
* Application Assessment
  + Application Scoring
  + Judgment
* Statement Printing
* Collection Inquiry and Entry
* Payment Acceptance
* Card Mailer Printing
* SMS Services
* Credit Management
* Customer Management
* Daily and Monthly Batch Process
* Interface File Generation
  + Customer Interface File
  + Account Interface File
  + Payment Interface File
  + Instalment Payment Interface File

1. **NEW FEP**

* HOST Interface to connect with HOST AS/400 module
* Stand-In Function to authorize transactions on behalf of HOST
* EMV Validation
* Process transaction messages to and from Brand Networks (Visa and MasterCard)
* New Infrastructure Model
  + Hardware and middleware, which is common to other countries, will be implemented, including the disaster recovery setup.

**Note:** Set up is subject for changes. ACSKH has to confirm this detail.

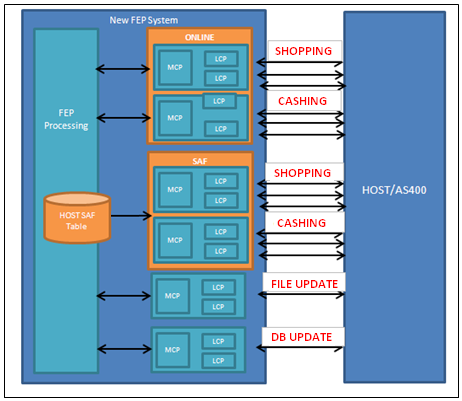
* New Monitoring System

1. **HOST**

* Judgment Interface
* Embossing
* Card Activation
* Pin Generation
* Sales Authorization
* Daily Settlement
* Daily Sales Closing
* Statement Interface Generation
* End Of Month (Month-End Closing)
* Payment Interface Processing
* Collection Interface Generation
* Card Installment Services
* Card Installment Management
* Card Blocking
* Annual Fee, Late Payment and Other Fees Charging
* Interest Calculation
* Minimum Payment Calculation
* Delinquency Aging
* Balance Management

**Note:** \* SMS will be subject to available technology partner of ACSKH

* + 1. NEW FEP Functions
       1. Host Interface



**Figure 2.4.1-A Host Interface Diagram**

The NEW FEP-Host Interface is composed of two components:

* **MCP** is responsible for checking/editing messages sent to and received from HOST. It will also be responsible for conducting Time-Out Monitoring.
* **LCP** is responsible for establishing socket connections between New FEP System and other external systems, such as HOST, VISA EA Server and others through TCP/IP protocol.

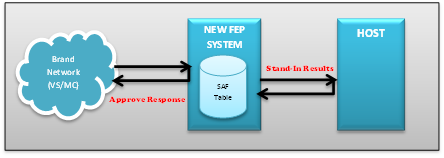
There are four types of port interfaces between NEW FEP and HOST:

1. **Online** – is the default interface for NEW FEP. It is responsible handling and processing online transactions.

There are two common types of online: Shopping for (EDC/POS) and Cashing (ATM).

* 1. Functional references to “Online” indicate an acquirer or issuer that is directly connected to the Card Brand Network, and does not imply any Web-based or Internet connotation.

1. **Store and Forward (SAF)** – responsible for Stand-In transactions and transactions that do not require HOST authorization.
   1. Stand-In Transactions: When NEW FEP system authorizes transactions in behalf of HOST (Stand-In), transactions authorized by NEW FEP pass through SAF port and are stored in a database designated for stand-in transactions (HOST SAF Table) until connection is established. Upon reconnection, all messages that were processed during stand-in will be forwarded by NEW FEP to Host. Hence the term “Store and Forward”.
   2. Transactions that do not require HOST authorization: Authorization Advice, Reversal Advice, and NEW FEP-Rejected Transactions.
2. **File Update** – responsible for HOST-initiated transactions like Manual Authorization, Account Update, etc.
   1. Issuers use Issuer File Update/03xx messages to block/unblock individual accounts from Card Brand Network level.
3. **Database (DB) Update** – responsible for Card Enrolment, CVV Generation, PIN Generation and other Card DB Update transactions (lost, stolen, hold).
   * + 1. Stand-In Function



**Figure 2.4.1-B New FEP System for STAND-IN Processing**

For Stand-In processing, transaction flow would be different from online processing. If a transaction encounters time-out (no response received from HOST) and reaches the maximum number of retries for sending an authorization message, referred to as “Maximum Send” count, Stand-In Function will be automatically activated. NEW FEP, instead of HOST will authorize the transaction, given user-defined criteria (e.g. Transaction Amount Limit, Transaction Count Limit).

At the same time, NEW FEP Store process will get the transaction message and save it on HOSTSAF table. If online connection is already established, NEW FEP Forward process will send the stored messages from HOSTSAF table to HOST. Messages stored in HOSTSAF will be deleted once the message was successfully forwarded. If the forwarding failed, it will be stored on the HOSTSAFBK (HOST SAF Backup) table.

Stand-In processing is only applicable for shopping transactions. Cashing transactions will automatically be declined by NEW FEP.

The New FEP System has a Stand-In function, where authorization is done in NEW FEP if HOST is not available.

New FEP System’s capability to check Stand-In transactions can be summed up as follows:

* + Can set amount limit for Stand-In. If the transaction amount exceeds the amount limit, then transaction will be declined. Amount limit and transaction limit for Stand-In transactions are all configurable. NEW FEP Administrator can manually change the limit in the Monitoring System.
  + Can set count limit. Count limit can also be updated in the Monitoring System.

Figure 2.4.1-C New FEP Stand – In Counter Flow Diagram shows how the Reconnection Counter works.

Scenario:

* + On the first transaction, HOST did not reply, thus, transaction was validated by NEW FEP through Stand-In Authorization and transaction counter value will be added by 1.
  + On the second transaction, NEW FEP will attempt to send Request message to online port. Still, no response received from HOST, so NEW FEP will validate again the transaction via Stand-In Authorization, and transaction counter will again increase to 1.
  + On the third transaction, HOST replied. Then validate the Request message and send a (0110) Response Message to NEW FEP.
  + Since the third transaction Request message was processed via online connection, transaction counter will not be incremented.
  + Stand-in transaction counter will reset upon going online.

The first two transactions will be forwarded to HOST via SAF, since Online connection is now available.

In case that the Transaction Counter reaches the Max Value\*\* (in the **Figure 2.4.1-C New FEP Stand – In Counter Flow Diagram** it’s 999), Stand-In processing will now be activated, and in order to switch to Online Mode, operator needs to do a manual switching via Monitoring System.

**Note:** \*\*Maximum Value (Max Value) for Stand-In Transaction Count depends on the hardware specifications and memory allocation for stand-in disk usage and the database setup.

External Network

FEP

HOST

Stand-In Transaction Counter

Max = 999

0100 Request Message

0100 Request Message

No Reply from HOST, will do Stand-In Authorization, Counter table on FEP will be added by 1

0110 Request Message

First Transaction Request Message

0100 Request Message

0100 Request Message

Will attempt to send Request Message to Online Gateway, but no Reply from HOST Online, so will do Stand-In Authorization, Counter table on FEP will be added by 1, current Counter table is 2

0110 Request Message

Second Transaction Request Message

0100 Request Message

0100 Request Message

FEP will attempt to send Request Message to Online Port. If FEP receives a response from HOST through Online port, FEP will forward the Transaction Request via Online connection.

0110 Request Message

Third Transaction Request Message

0110 Request Message

On the First Transaction, counter will be added by 1. On the Second Transaction, counter value will become 2. On the Third Transaction, there's a Response received from HOST Online, message will now be validated by HOST. The next transaction will now process or send to online connection. Counter will reset upon going online.

**Figure 2.4.1-C New FEP Stand – In Counter Flow Diagram**

* + - 1. EMV Validation

**HOST**

6Approve Response

5

3

4

7

2

8

1

**FEP**

**EDC (NON-AEON)**

**BRAND NETWORK**

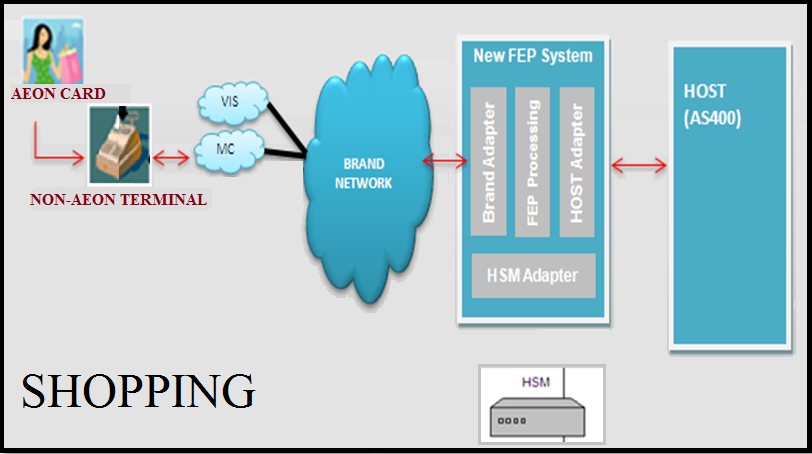
**HSM**

**Figure 2.4.1-D EMV Validation Diagram**

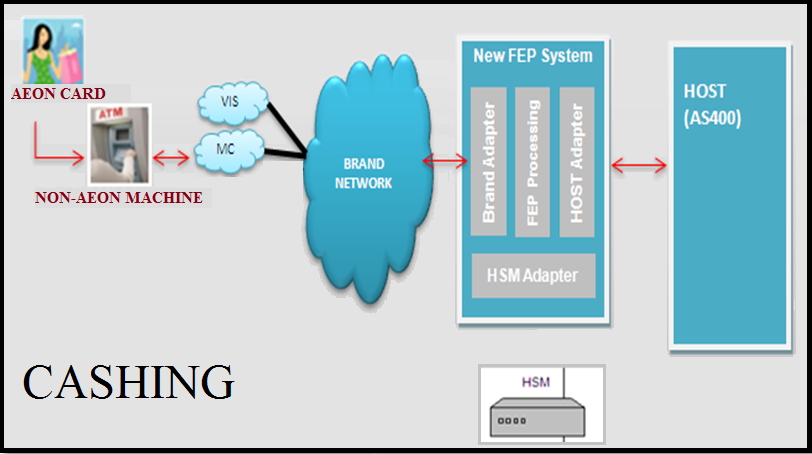
EMV (Europay MasterCard VISA) Validation is another feature of New FEP System. The new System has a capability to support and do authentication checking for Integrated Chip (IC) transactions received using the standards defined by EMVCo.

Figure 2.4.1.3 EMV Validation Diagram shows how New FEP System validates IC data is illustrated.

1. IC Chip Read (Request EMV Data [ARQC]) will be forwarded to Brand Network.
2. Authorization Data (Including EMV Data) will be forwarded to NEW FEP.
3. EMV data will be forwarded to HSM (ARQC Validation and ARPC Generation will be done).
4. ARQC Result and ARPC will be sent by HSM to NEW FEP.
5. If transaction is approved, Request Message will be forwarded to HOST.
6. HOST will send Response Message back to NEW FEP.
7. NEW FEP will send response message to Brand Network.
8. The result of the transaction, including EMV validation will be forwarded to the Electronic Data Capture Terminal (EDC Terminal).
   1. **ISSUING Transaction Flow**



**Figure 2.4.1-E Shopping Transaction through Card Brand Adapter**



**Figure 2.4.1-F Cashing Transaction through Card Brand Adapter**

For Issuing transactions, AEON card will be used on a Non-AEON terminal/merchant. Transaction requests will be forwarded to NEW FEP from the Card Brand network. Brand Network Adapter will receive the request then forwarded to NEW FEP Processing for basic checking. NEW FEP Processing will forward CVV/iCVV/IC data and PIN (for cashing transactions) for HSM checking. If request message passed the NEW FEP basic checking then request message will be sent to HOST for balance/credit checking. HOST will send back a response message to NEW FEP. NEW FEP will send back the response message to Brand Network up to the terminal/merchant.

* + - 1. Middleware

Middleware included on NEW FEP Servers are the following:

* 1. **Interstage**
     1. Core - web service and inter-process communication within FEP System.
     2. JMS - provides the inter-process communication function in FEP system.
     3. IJServer - manages the WEB Application (Servlet / JSP. Etc.)
  2. **System Walker Centric Manager** - detects if errors were encountered in NEW FEP System. Sample errors detected by System Walker Centric Manager:
     + Line Disconnection
     + Database Error
     + Unusual Declined Transaction (Constant PIN and CVV/ICVV/CVV2 – HSM Error)

**Note**: Operators can be notified by the following methods:

* + - Error Lights
    - Send E-Mail (SMS)
    - Through Management Console
  1. **System Walker Operation Manager\*\* -** is responsible for setting and running Batch Jobs. Below are the sample Batch Jobs operated by System Walker Operation Manager:
     + Log Deletion and Data Clear
     + System Startup
     + System Shutdown
     + BIN Table Update
     + Process Status Collection
     + ATM Key Exchange
     + Sign-on/off
     + Operation Log Transmission
     + EDC Settlement Data Transfer By Schedule
     + Echo Test Message Request
     + Data Synchronization Transmission
     + Data Synchronization Import
     + EDC Settlement Data Transfer By Screen
     + Shared Memory Clear
     + Symfoware Sequence Reset

**Note: \*\*** Out of the scope for the first phase of the ACS-KH Credit Card Systems Project.

* 1. **Primecluster HA Server -** detects abnormality (exceptions/errors) rapidly and correctly in order to make sure that the server operates without interruptions.
  2. **Primecluster GLS** - provides network redundancy and communication with high reliability (the operation can continue processing even if network path is offline or down). Since this software can change the route automatically
     1. Monitoring System Functions

New Monitoring System (MonSys) will be part of the New FEP System. The MonSys Project includes the three major monitoring functions such as System Monitoring function, Service Monitoring function, and Report function.

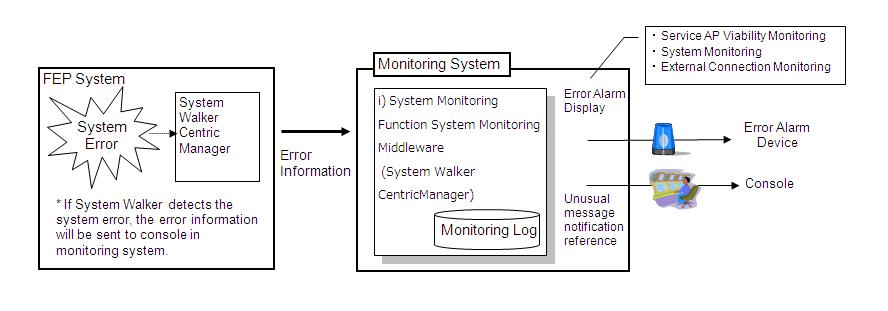
* **System Monitoring Function** – Monitors service application viability of the NEW FEP System, hardware, external connections with the NEW FEP system, and data synchronization (data synchronization between main site and disaster site).

This function is handled by SystemWalker Centric Manager of Fujitsu**\*\***.

* **Service Monitoring Function** – has browsing functions for transactions (EDC/All Brand Transactions) that occur through the NEW FEP system. Manages the master data such as AEON BIN data, network sign on/off and user account.

**Note:** Monitoring System will only be able to display a transaction AFTER the transaction cycle has been completed in NEW FEP.

* **Report Function** – Generate reports such as transaction summary and transaction proof list.
  + - 1. **System Monitoring Function**

**Figure 2.4.2-A System Monitoring Function Diagram**

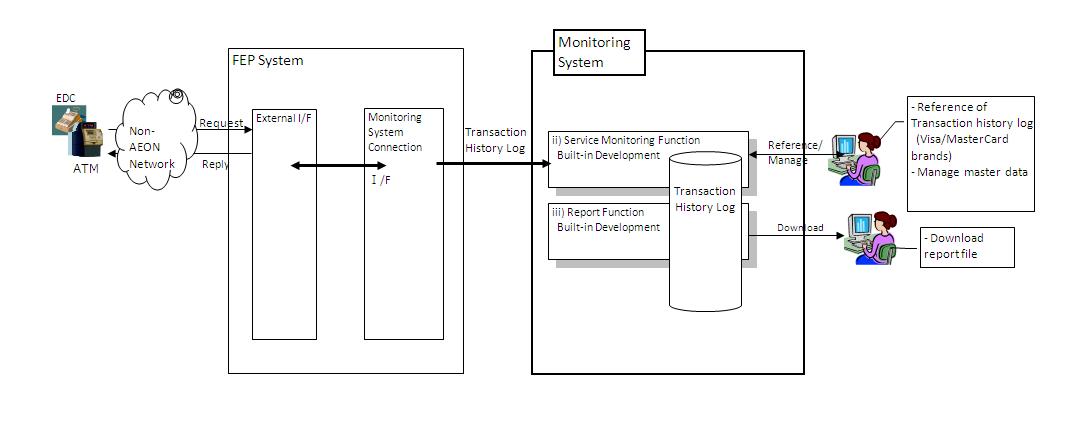
The System Monitoring Function is implemented using the SystemWalker Centric Manager of Fujitsu.

The SystemWalker Centric Manager monitors and detects errors encountered in the New FEP System. Sample errors detected by the SystemWalker Centric Manager are as follows:

* + - * Line disconnection
      * Database error
      * Unusual declined transaction (Constant PIN and CVV/ICVV/CVV2 – HSM error)

The operators will be notified via “Error Lights” or through SystemWalker Management Console. The line disconnection/declined transaction can also be viewed in [Network Status Query](#_FUNC2.3.1_Network_Status) / [Transaction History Live](#_FUNC2.1.1_Transaction_History) screens of FEP Monitoring System.

* + - 1. **Service Monitoring Function**

****

**Figure 2.4.2-B Service Monitoring Function Diagram**

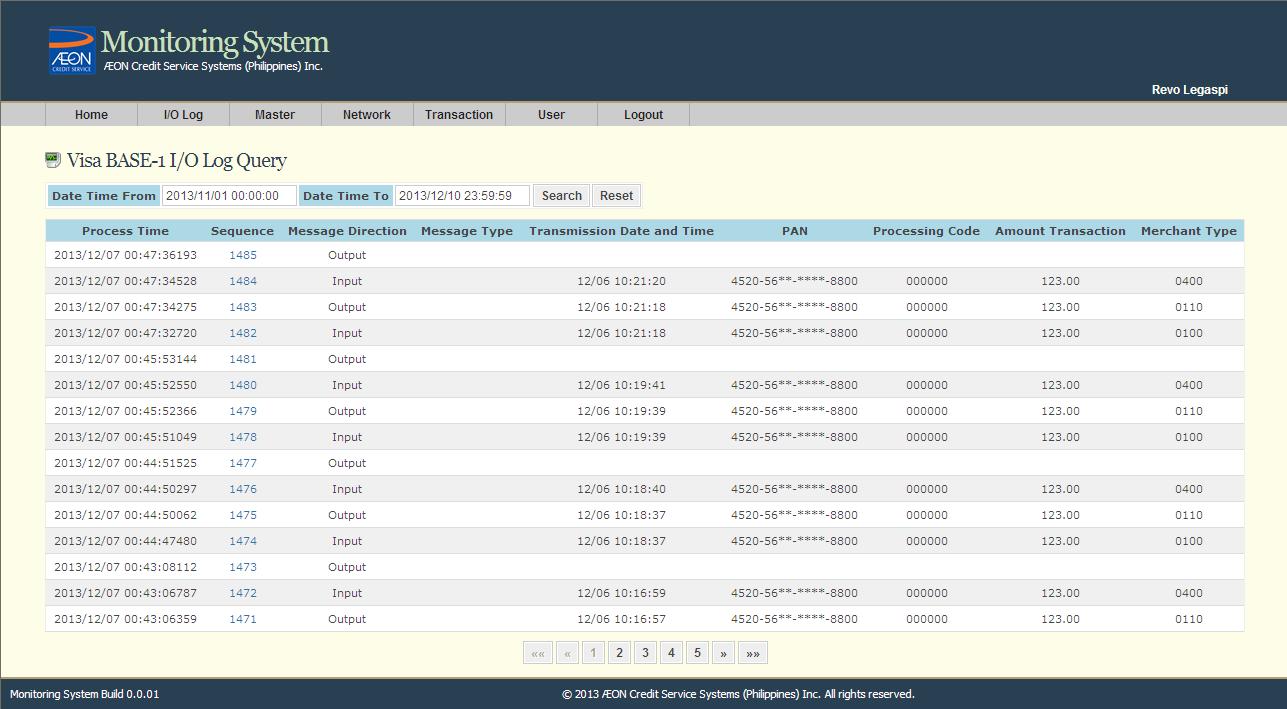
The Service Monitoring Function focuses on the following:

1. **IO Log**

This is used for viewing IO Logs from different Network Connections that the New FEP System received and sent. User can access the different IO Log Screens under the IO Log Tab.

IO Log screens are the following:

* Authorization I/O Log Query
* MasterCard BANKNET I/O Log Query
* Host I/O Log Query
* HSM I/O Log Query
* Visa BASE-1 I/O Log Query

**Figure 2.4.2-C MS – I/O Log Query**

The Visa BASE-1 I/O Log Query is used for viewing Visa I/O messages received by NEW FEP from Visa and vice versa

\*Please refer to FEP ACS-KH-MONSYS-Functional Requirements Specification v1.00.docx for other IO Log Screens.

1. **Master**

The FEP Monitoring System has the function to manage the NEW FEP master data such as:

* + BIN Maintenance
  + Card Account Query (View only)
  + Card Type Maintenance
  + Customer Type Maintenance
  + DESKEY Table Maintenance
  + Merchant Type Maintenance
  + PAN Country Code Maintenance
  + POS Entry Mode Maintenance

These data are used for:

* + Stand-in transaction authorization
  + Security verification for PIN, CVV, CVV2, ICVV, and IC Data
  + AEON/Non-AEON member card identification

1. **BIN Maintenance**



**Figure 2.4.2-D MS – BIN Maintenance Query Screen**

The BIN Maintenance is for viewing the list of AEON/Non-AEON BINs (with add, update, and delete functions). The BIN table is updated during the scheduled BIN synchronization between the NEW FEP and HOST.

\*Please refer to FEP ACS-KH-MONSYS-Functional Requirements Specification v1.00.docx for other Maintenance Screens.

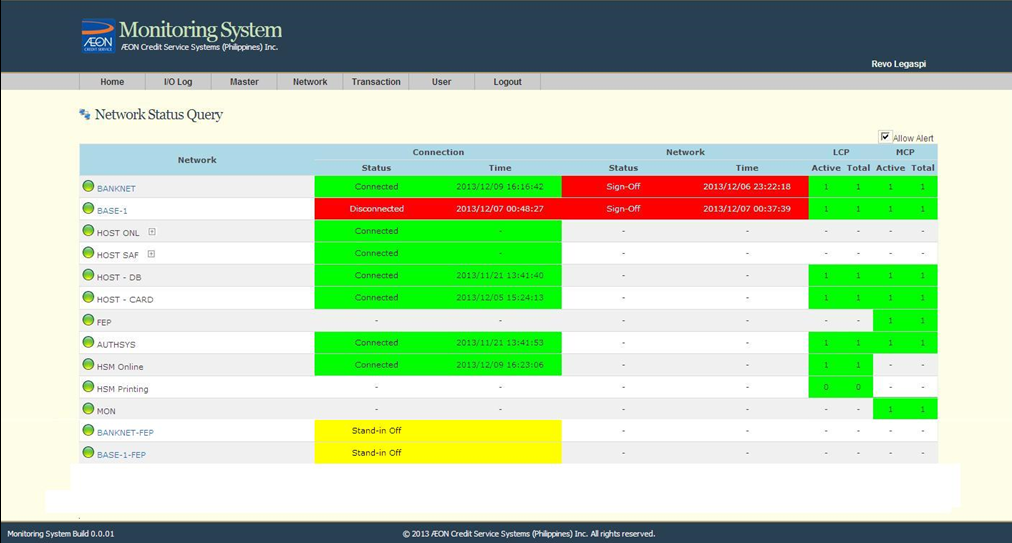
1. **Network**

This module monitors the connectivity status and queue status of the External I/F connections. When a user opens the Network Status Query/Network Status screen, it will retrieve the information from the system and will be shown on the screen.

When user performs the “Sign-on”, “Sign-off” or “Echo Test” for specific card brand in the Network Control Maintenance screen, the NEW FEP Monitoring System will send the command to SystemWalker for processing. The SystemWalker will then send the command to the corresponding External I/F connection.

Screens under network tab are the following:

* + - Network Status Query
    - Network Queue Status Query
    - Network Control Maintenance



**Figure 2.4.2-E MS – Network Status Query Screen**

The Network Status Query is for viewing connection status and stand-in status of every external network. A sound alert notification will inform the operator when there is an abnormal (red) status shown in the list.

\*Please refer to FEP ACS-KH-MONSYS-Functional Requirements Specification v1.00.docx for other screens.

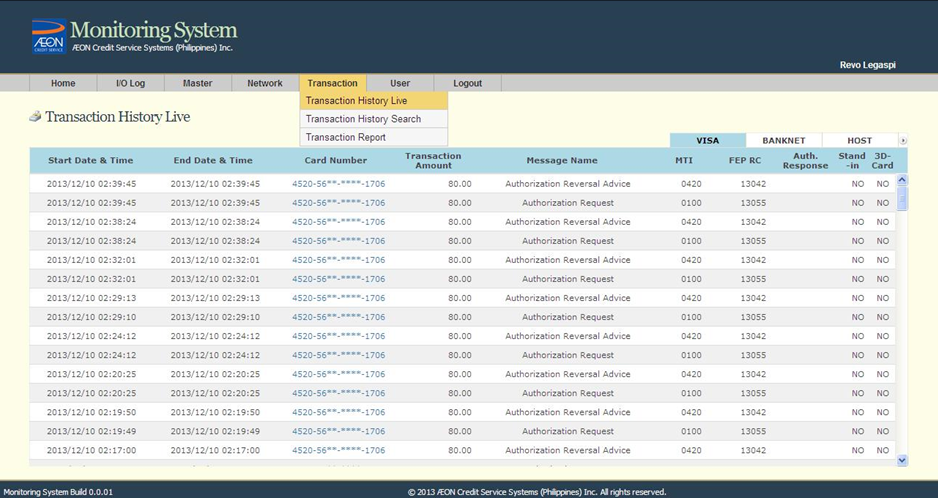
1. **Transaction**

Upon receiving transaction from EDC Terminals (Issuing) and Host, the transaction will be processed by New FEP system and will send it to Monitoring System.

The transaction could be displayed in the Transaction History Live screen of NEW FEP Monitoring System.

The user may view/search the transaction using the following screens:

* + Transaction History Live



**Figure 2.4.2-F MS – Transaction History Live Screen**

* + Transaction History Search

The Transaction History Live Screen is used for viewing of transactions processed by the New FEP System in real-time. The most recent transaction is displayed at the top of the list.

The transactions are grouped by the following tabs:

VISA – Listing of issuing transactions coming from VISA.

BANKNET – Listing of issuing transactions coming from Master Card.

HOST – Listing of transactions coming from Host.

\*Please refer to FEP ACS-KH-MONSYS-Functional Requirements Specification v1.00.docx for other Transaction Screens.

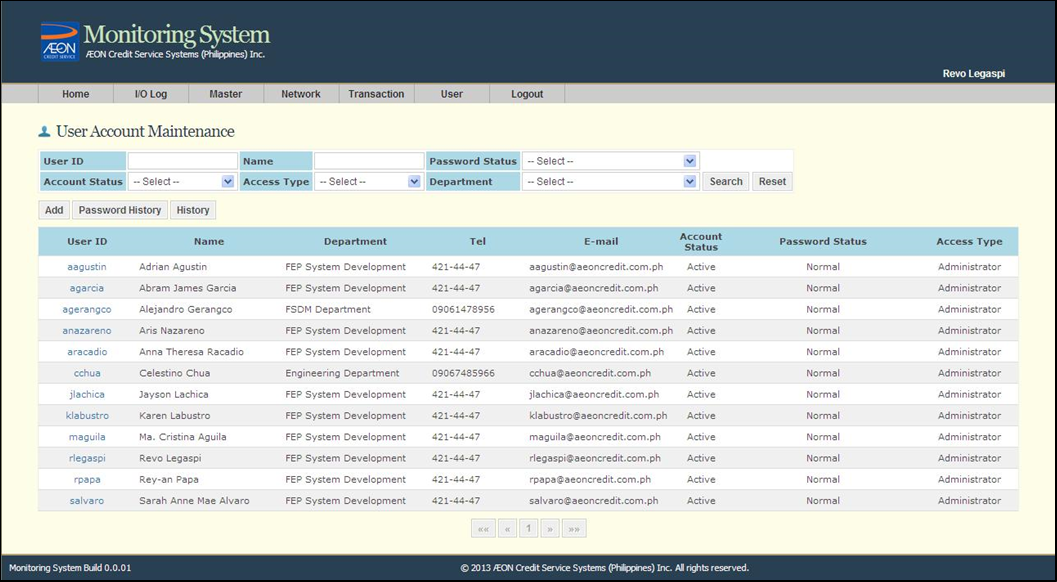
1. **User**

The NEW FEP Monitoring System has functions to manage the Monitoring System User Account such as:

* Password Change
* User Account Query and Maintenance
* Department Master Maintenance
* Login Record Query
* Authority Maintenance
* User Session Control Query

This function group is used for:

* Monitoring System users registration
* Online user password maintenance
* Department list registration and modification
* User login activities monitoring
* Setting the authorities right for role group of the Monitoring System
* Monitoring user session

****

**Figure 2.4.2-G MS – User Account Maintenance Screen**

The User Account Query and Maintenance is for adding, modifying and deleting user accounts. User can reset passwords and search registered users.

\*Please refer to FEP ACS-KH-MONSYS-Functional Requirements Specification v1.00.docx for other screens.

1. **Report Function**

The Report function enables the user to view some information or analysis on the transactions. The report can be on a CSV (Comma Separated Values) file or an XLS (Microsoft Excel) file that can be downloaded from or viewed on the Report Creation Screen.

The user may download the reports using the Daily Transaction Report under Transaction Tab.

* 1. **Daily Transaction Report**



**Figure 2.4.2-H MS – Daily Transaction Report Screen**

The daily report creation is for generating daily transactions per Card Brand.

The generated Excel report file will contain the following tabs:

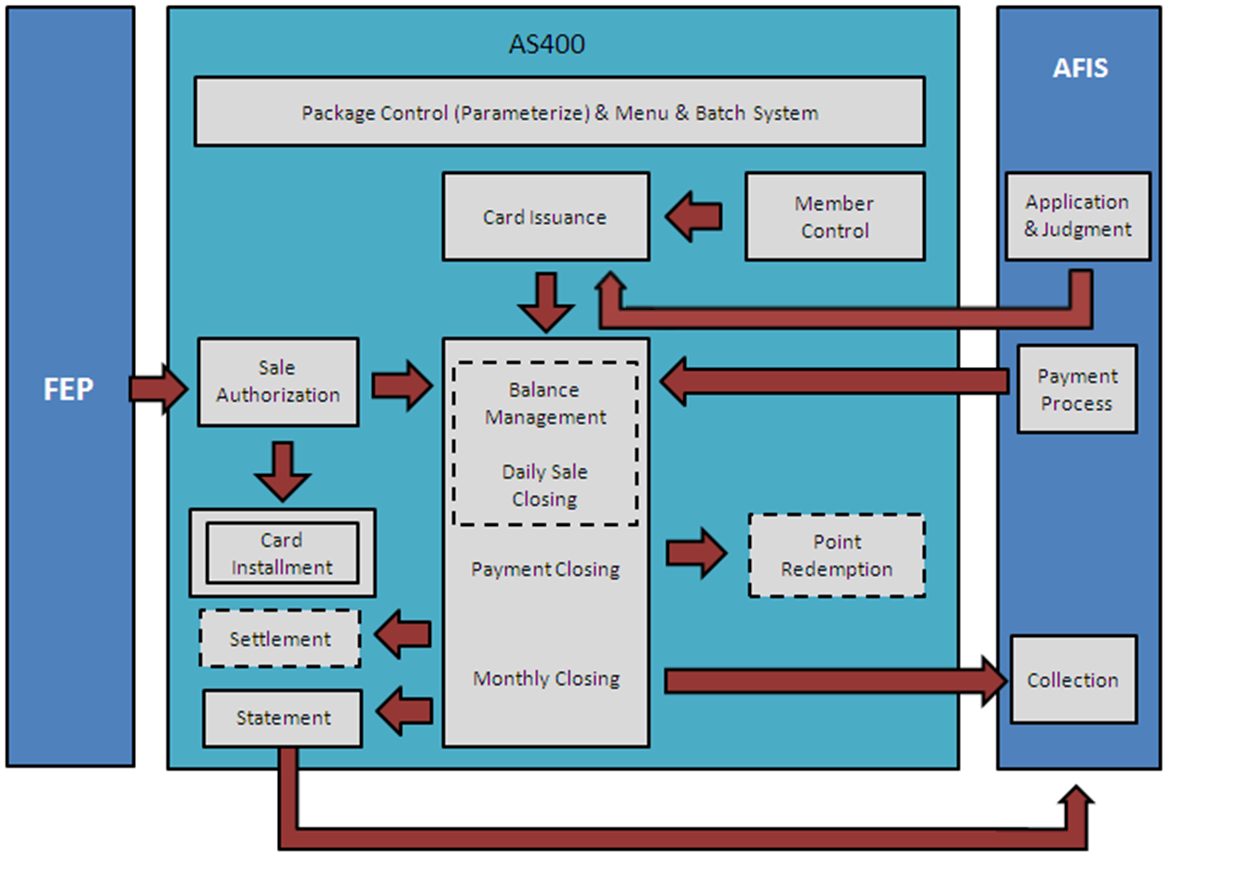
* Total Transaction
* Hourly Transaction Chart
* Response Code Summary
* Merchant Summary
  + 1. HOST Functions

**Legend:**

* (Arrow Heads) pertain to the actual flow of interface files between each function in the HOST System.
* Functionalities enclosed in dashed boxes are already implemented in ACSI Credit Card System.



* Functionalities enclosed in double lined boxes are new functionalities.



**Figure 2.4.3 HOST Functions Diagram**

* **Member Closing**

This is the process of assigning of a Credit Card Number and Expiration date on the customer’s credit card account.

* **Card Embossing**

This is the process of personalizing the customer’s card. Customer’s information and other security data will be stored in the credit card.

Example: Card Number, Expiration Date, CVV1, CVV2, iCVV (for chip cards only).

* **PIN Generation**

This is the process of generating and printing random PIN to be sent to the cardholder. This is necessary for Cash Advance Transactions.

* **Card Activation**

This is the confirmation of the card holder for receiving the credit card. Customer Service asks for personal information regarding the Cardholder to confirm the ownership of the account. If card activation is successful, the customer can already use the credit card.

* **PIN Change**

This is the process of changing the PIN of the credit card from random PIN (cardholder will receive a PIN Letter from the Issuing bank) to the new personalized pin. Most issuing banks require this before the card can be used in Cash Advance Transaction.

* **Authorization (Sale/Cash Advance)**

This is the process of receiving and validating credit card transaction from VISA and MasterCard. The Issuer will reply with an approved or rejected response depending on the result of the verification.

* **Settlement**

The acquirer sends the batch transactions thru VISA and MasterCard, which debits the issuers for payment and credits the acquirer. Essentially, the issuer pays the acquirer for the transaction.

* **Sales Closing**

This process ends the Sales month in which the transactions within the sales month will be billed in the next billing after Payment Closing.

* **Statement Generation (Billing)**

This process is done after the Sales Closing. The system will generate billing file and converted to a Billing Statement for each customer to be sent in their billing address.

* **Monthly Closing**

This is the process of summarizing all the sales authorized against the payments received by the Credit Card Issuer for the entire financial month. Statistics are generated to check the collection/un-collection report of the Issuer.

* **Re- Presentment/Chargeback**

Chargeback is typically initiated by the cardholder. In the event of a successful [chargeback](http://en.wikipedia.org/wiki/Chargeback), the issuer returns the amount to the acquirer for resolution. The acquirer then forwards the chargeback to the merchant, who must either accept the chargeback or contest it.

Re-presentment is a chargeback that is rejected and returned to a card issuer by the merchant’s processing bank on the merchant’s behalf. A chargeback may be re-presented, or re-deposited, if the merchant or the processing bank can remedy the problem that led to the chargeback. To be valid, a re-presentment must be in accordance with regulations established by Visa and MasterCard and to be submitted within the specified time frame. The two Credit Card Associations have the final say as to the validity of a chargeback or a re-presentment, if the two affected banks cannot resolve the issue between themselves.

**Note:** A chargeback is an event in which money in a merchant account is held due to a dispute relating to the transaction.

* + 1. AFIS Functions

Legend:

* (Arrow Heads) pertain to the actual flow of interface files between each function in the AFIS System.
* - Functionalities / Process / Activities being performed by each actor

**Customer**

**AFIS**

Application Scanning

Captures Application Information

Application Assessment

Daily Batch Run

**AS 400**

Statement

Monthly Batch Closing

Payment

Application

Daily / Monthly Closing

Credit Management

Payment Acceptance

**Figure 2.4.4 AFIS Functions Diagram**

* **Application Scanning**

This is the process of converting the hardcopy of the documents submitted by the Customer into an electronic copy. This is where the system also groups the documents by Applicant.

* **Captures Application**

This is where the information defined in the electronic document (application form) is encoded into the system.

* **Application Assessment**

The process where the application will be evaluated and judged based on the given information. Some of the things that will be considered during judgment would be the following items:

* Credit scoring
* Negative information
* Duplicate check
* **Payment Acceptance**

Payments made by the Customer will be captured using any of the following:

* Counter Payment
* Bank Payment (Upload)
* Collector Payment
* **Daily Batch Run**

At the end of day, the daily batch will be executed. Information regarding new Account, update on customer’s records and payments will be processed and will be transferred to the HOST system for record synchronization.

* **Monthly Batch Closing**

During month end closing, AFIS will run the Monthly batch closing to extract the outstanding balance from the HOST system. The outstanding balance will then be used by AFIS for account allocation. Information regarding billing statement will be extracted also for printing.

* **Credit Management**

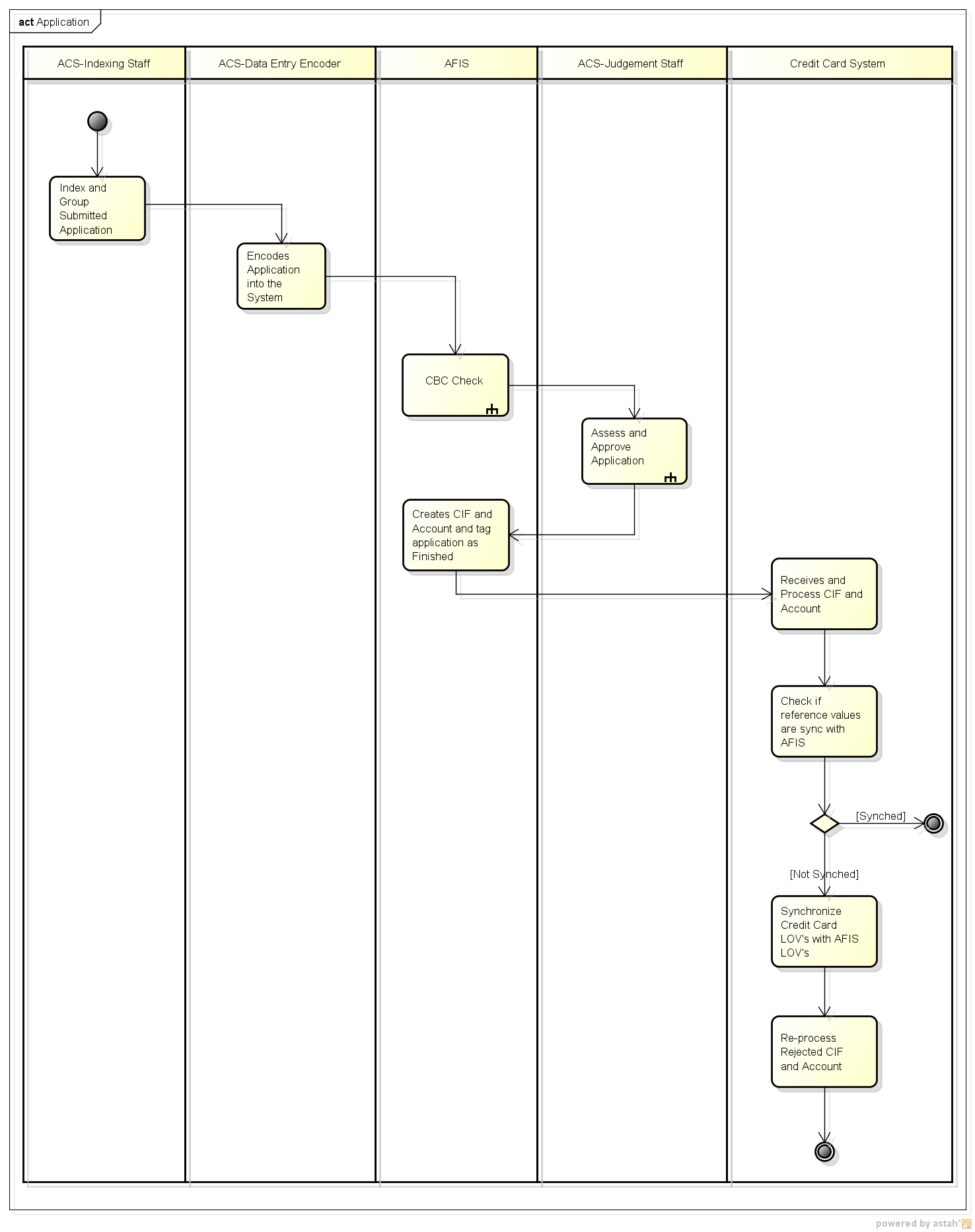
All Agreements (HP and Credit Card Sales) due for payment will be allocated to the desk collector for payment follow up.

# FUNCTIONAL REQUIREMENTS

For the ACSKH Credit Card System the following transactions will be rolled out on Phase 1:

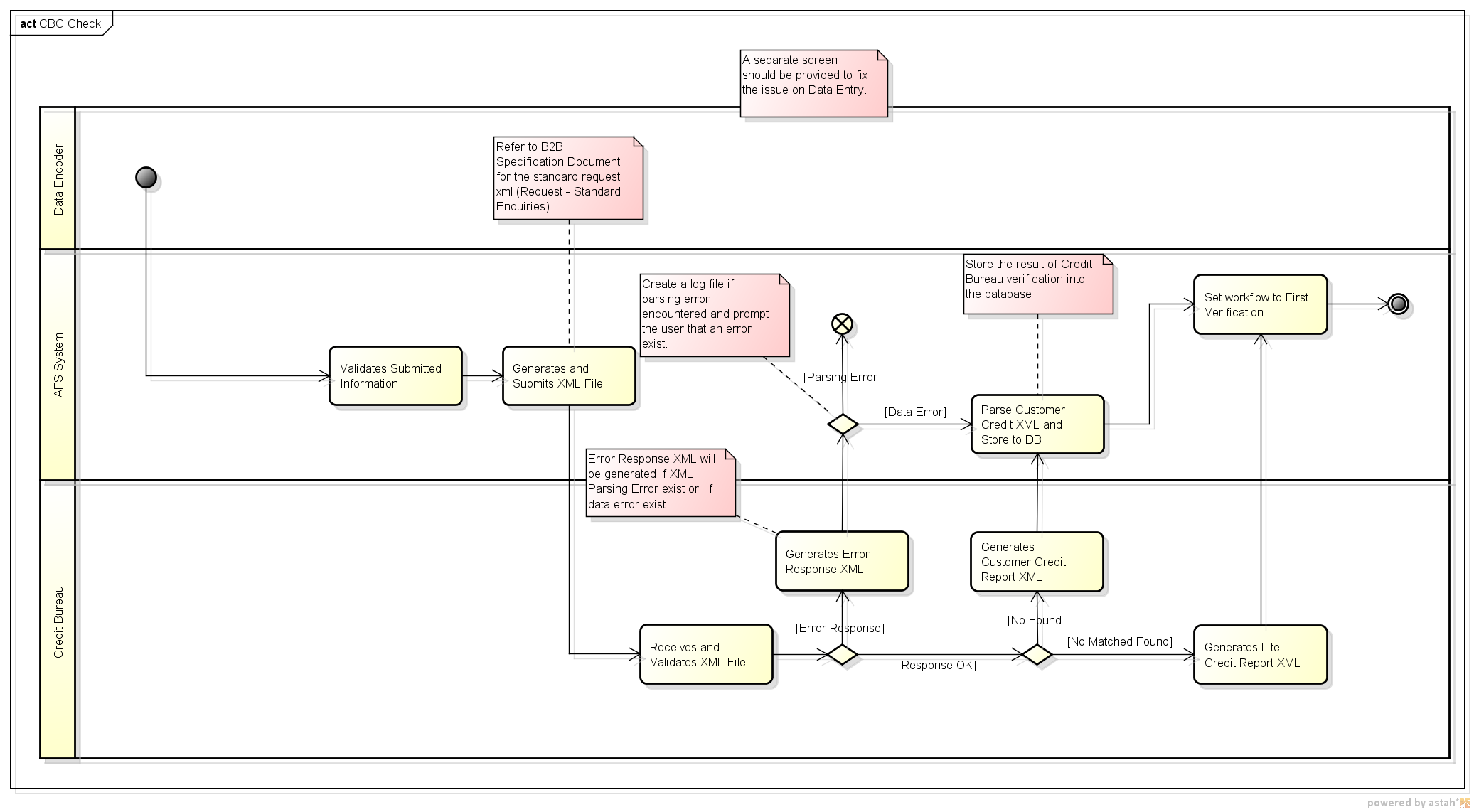
1. Visa Issuing Transactions
2. Master Card Issuing Transactions

## FR001 Application Process



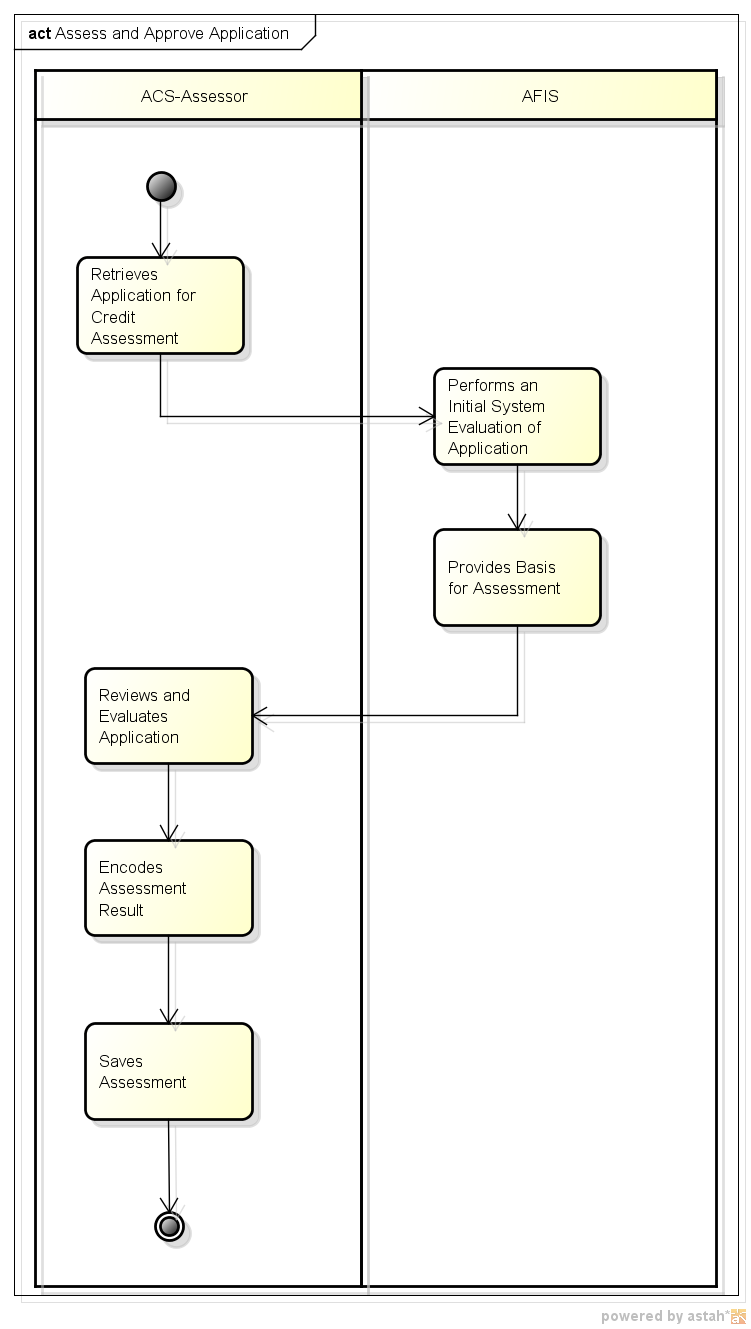
|  |  |
| --- | --- |
| **Overview** | The application process is the first step of the Credit Card process. At this stage, the applicant submits the application form and other documents required to the branch, by mail, by fax, agents, or through partner merchants. |
| **Pre-condition** | Prior to Application, Applicant should have the following:   1. Two (2) Valid government IDs for Identification: Driver’s License, Passport or other government issued ID 2. Proof of income  * Proof of Salary or payslip, Bank Statement   **The Credit Card Application may be observed as follows:**  **Agent**   1. *Distributes Credit Card Application Forms to Applicant.*   **Applicant**   1. *Accomplishes Credit Card Application Form.* 2. *Submits the Application Form and Supporting Documents.*   **Agent**   1. *Receives and forwards the Application Form and Supporting Documents.*   **Note**: Actual Card Application process is subject to change according to ACS-KH’s discretion*.* |
| **Process** | **ACS-Indexing Staff**   1. Group the documents submitted by applicant    1. *If documents submitted are incomplete, contact the applicant.*    2. *If documents are complete, application will be forwarded to Data Entry Staff to data information capture.*   **ACS-Data Entry Staff**   1. Based on the submitted application form, the data entry staff encodes the information provided into the system.   **AFIS**   1. Encoded information provided will be used to perform an online credit bureau check. The AFIS system will perform an online query to check if applicant has a bad credit bureau record. 2. Result of CBC will be stored and can be used to assess the application   **ACS-Judgement Staff**   1. Judgement staff will assess the application based on the following:    1. *Negative Information*    2. *Scoring*    3. *Result of CBC*   *Note: Refer to Assess and Approve Application Process for Detail*  **AFIS**   1. A corresponding CIF and Account file will be created for approved application and will be forwarded to the Credit Card System end of day.   **CCS**   1. Receives and process CIF and Account File 2. Determine if CIF and Account contains unmatched reference data   **ACS-Admin**   1. If there is an unmatched reference data, System administrator needs to perform manual synchronization of data. 2. Performs a re-processing of CIF and Account once data sync is complete. |
| **Result** | Applicant information is stored into the System. |
| **Remarks/Note** | * When all requirements are completed and verified, the information will serve as input in the Data Application Entry |

* 1. **FR001A CBC Check**



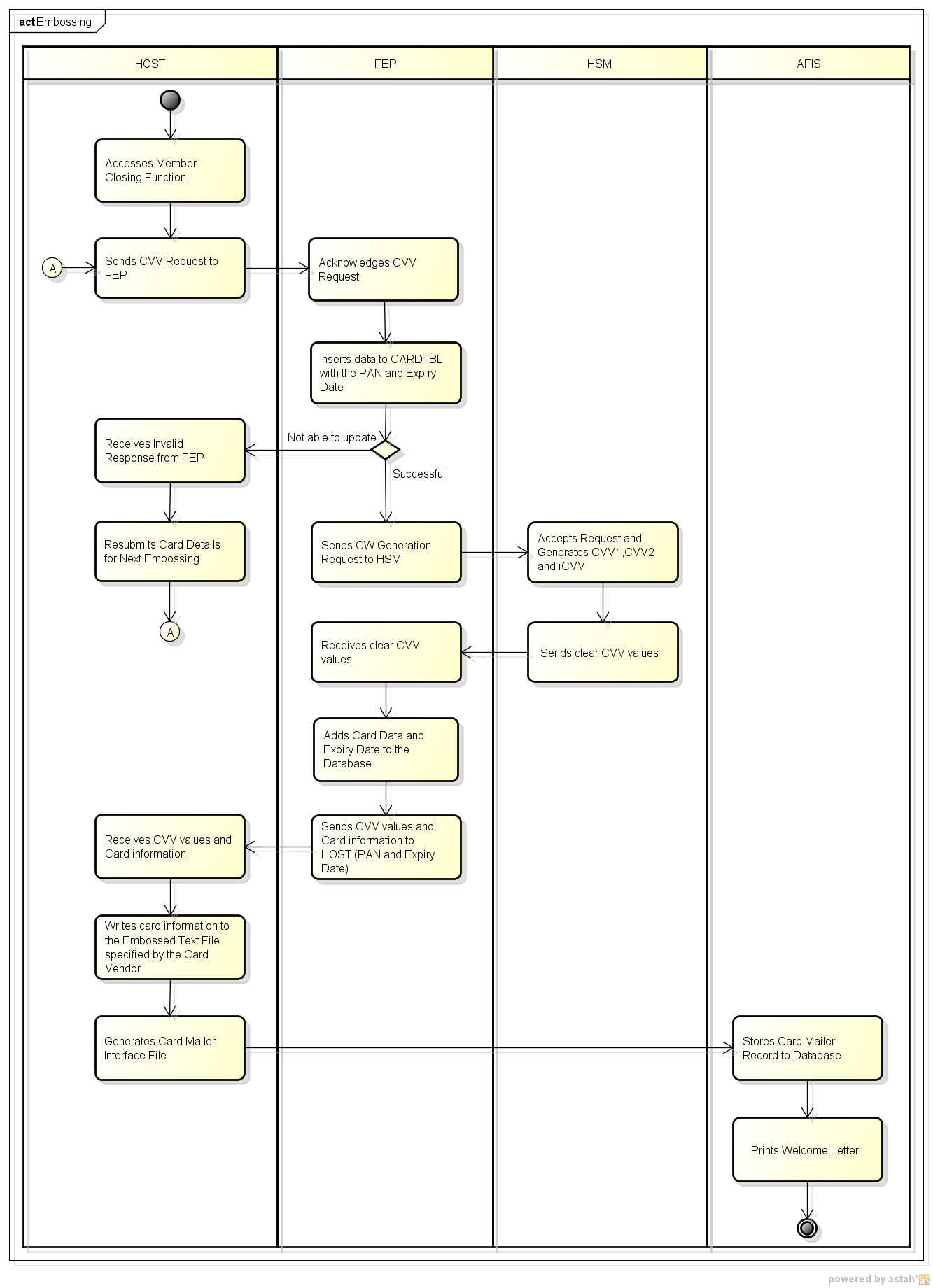
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Overview** | The CBC offers a Consumer Inquiry Report that will provide details to the Assessor to help them to make an informed credit decision. The information which will be provided to Assessor will help them manage the following:   |  | | --- | | - Credit Risk | | - Fraud Monitoring | | - Check credit report or credit standing of applicant | | - Check Applicants Identity | |
| **Pre-condition** | All required information needed to perform a CBC check are available. |
| **Process** | **AFIS System**   1. Validates the encoded / Submitted Information. 2. Generates and Submits XML File. If the encoded information is valid, system will generate a corresponding XML file and the xml file will be submitted to the Credit Bureau.   **Credit Bureau**  1) Credit Bureau receives and validates the XML file and check for any issue.   * It will check for a parsing or data error and will produce a response XML if there is. * Generates a Customer Credit Report XML if no record exists in the Credit Bureau DB. * Generates a Customer Credit Report Lite XML if record exist in the Credit Bureau DB.   **AFIS System**  1) Checks for the type of XML returned by Credit Bureau.   * If parsing error exist, System will record the error in the application log. * If Data Error or record found, System will create Credit Verification record and will set the status for credit verification. * If no matched found, system will forward the application for Credit Assessment. |
| **Result** | Possible Results:   * Parsing or Data Error * Record of Customer does not exist in Credit Bureau * Record of Customer exist in Credit Bureau |
| **Remarks** | * AFIS might do an online interface with Credit Bureau to perform a CBC Verification |

* 1. **FR001B Assess and Approve Application Process**



|  |  |
| --- | --- |
| **Overview** | This is the process of evaluating the information provided by the customer in his/her application and decide if he/she is credible to have a credit card.  Evaluation of Customer Application can be done in the Credit Assessment module.  This is also the process wherein it is decided what Credit Limit (Both for Credit Purchase and Cash Advance) is to be applied for the customer. |
| **Pre-condition** | All requirements based on the Credit Card Application have been provided already by the applicant. |
| **Process** | **ACS-KH Assessor**   1. Retrieves the application he wants to evaluate   **AFIS**   1. Performs an automated evaluation of the application 2. Provides all the information necessary for the assessor to conduct his assessment.    1. Calculate the Credit Limit    2. Provides the Credit Scoring    3. Notify the assessor if there are documents that needs to be submitted    4. Provides Negative Information about the customer    5. Provide information with regards to duplicate applicant records.   **ACS-KH Assessor**   1. Reviews and evaluates the application. Reviews and evaluation is based on the information submitted by the applicant and the provided assessment recommendation by the system. 2. Saves the assessment result |
| **Result** | Possible Results of the Judgment Process:   * Approved – Applicant is credible to have a credit card * Declined – Applicant is not credible to have a credit card * Cancelled – Applicant decided not to continue his/her Credit Card Application * Verification – If further information is needed in order to proceed with the assessment. |
| **Remarks** | * Judgment process should commence after Card Application Process. * Company policies for Assessing Application Requirements will be applied (e.g. Background Checking of Applicant and verification of submitted documents). * Company policies for Application Scoring will be applied (e.g. Points Policy, Collection History). |

## FR002 Embossing Process



|  |  |  |
| --- | --- | --- |
| **Overview** | This is the process where generation of CVV values takes place. This is the process of personalizing the customer’s card. Customer’s information and other security data will be stored in the credit card. For example, Card Number, Expiration Date, CVV1, CVV2, and iCVV. | |
| **Pre-condition** | * Member closing was already performed. * Established subsystem connection between HOST and NEW FEP, as well as HSM and NEW FEP. * CVK value is stored in New FEP. * Embossing machine should also have the MDK for IC. | |
| **Process** | **HOST**   1. Accesses Member Closing function 2. Sends CVV request to NEW FEP   Message Request should contain the following details:   * 1. PAN   2. Expiry Date   **NEW FEP**   1. Acknowledges CVV request 2. Inserts date to CARDTBL with the PAN and Expiry date. 3. If unsuccessful, sends invalid response to HOST. 4. If successful, sends three CVV generation requests to HSM for the following    1. CVV    2. CVV2    3. iCVV   **HOST**   1. If CARDTBL update is unsuccessful, resubmits card details for next embossing.   **HSM**   1. Accepts request and generates CVV, CVV2 and iCVV values one after the other. 2. Sends clear CVV values to NEW FEP.   **NEW FEP**   1. Receives clear CVV values. 2. Adds card data and expiry date to the database. 3. Sends CVV values and card information to HOST   **HOST**   1. Receives CVV values and card information 2. Writes card information to the embossed text file specified by the card vendor. 3. Generates Card Mailer Interface File   **AFIS**   1. Stores Card Mailer Record to Database 2. Prints Welcome Letter |
| **Result** | * Approved – Successful update to CARDTBL and CVV generation. * Declined – Unsuccessful update to CARDTBL and CVV generation. |
| **Remarks** | Unsuccessful CVV generation will be sent on the next embossing schedule. |

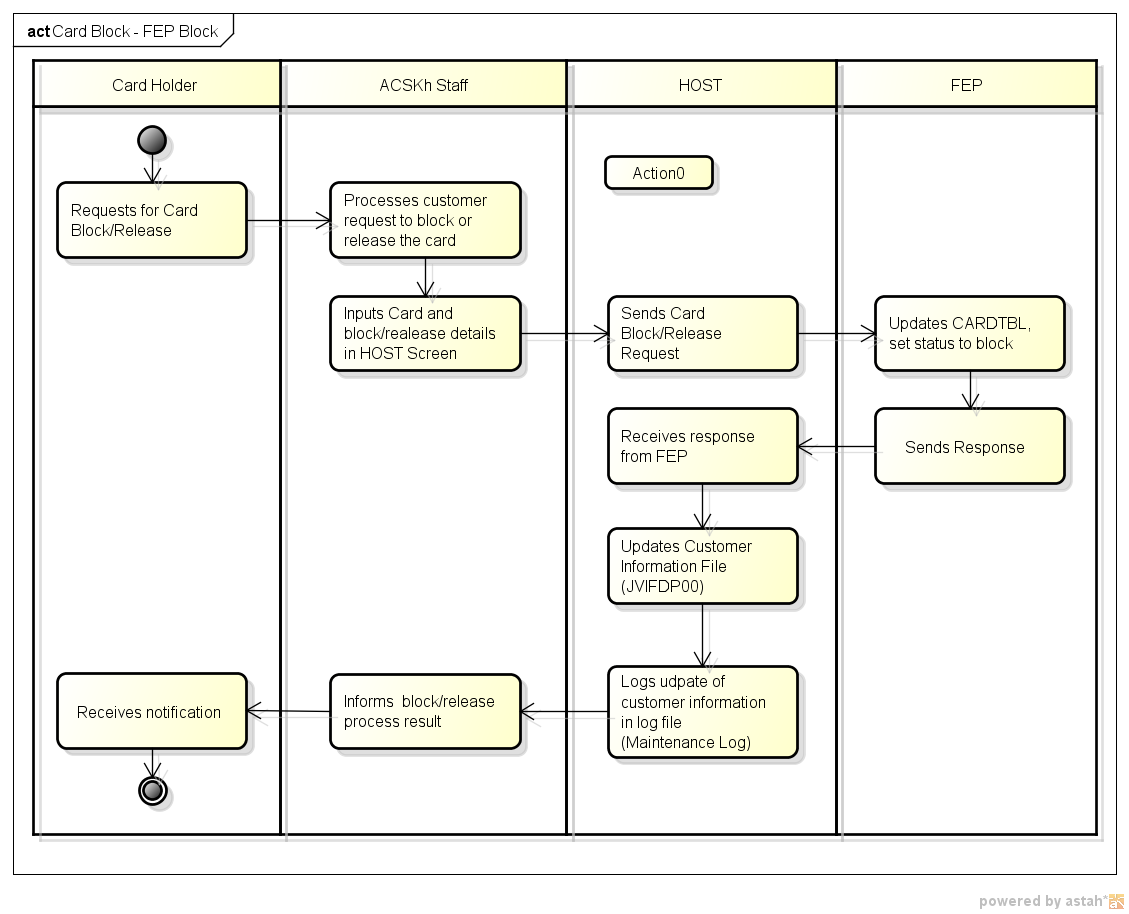
## FR003 Card Activation Process

**FR003A Manual Activation (Call-Center Activation/Branch Activation)**

|  |  |
| --- | --- |
| **Overview** | This is the process where cardholder activates the card for transaction. In this process, cardholder confirms that he/she received his card. Card Activation is done in order to allow the cardholder to make sales transactions with his/her card. Card status in the master file is changed from “1” – Embossed to “2” – Card Activated |
| **Pre-condition** | * Credit Card is already in cardholder’s possession. * Customer service/Branch staff has the authority to activate card. * Card holder requests to activate his/her card. * For Card Activation, the following details should be known to the card holder:   1. Credit Card Number   2. ID Number |
| **Process** | **HOST Operator**   1. *Validates if provided details by cardholder is correct or not.* 2. If cardholder details are not valid,    1. *Notifies card holder.*    2. *Declines card activation.* 3. If cardholder details are valid,    1. *Activates the card through HOST screen*.   **HOST**   1. Sends card activation update status to NEW FEP.   **NEW FEP**   1. Receives HOST’s request and validates the card’s existence in the database. 2. If Card Check is OK    1. Updates card table and change to ‘Normal’ status.    2. Sends acknowledgment reply to HOST. 3. If Card Check is NOT OK.    1. Sends message to HOST.   **HOST**   1. Receives reply from NEW FEP. 2. If Card Activation is successful,    1. Updates Card Status from “Embossed” to “Activated”.    2. Notifies the cardholder. 3. If Card Activation is unsuccessful,    1. Goes back to Embossing Process.   **HOST Operator**   1. Receives notification thru the HOST Screen that card has been activated. 2. *Notifies Cardholder that card has been activated.* |
| **Result** | If card activation is successful, the cardholder can already use the credit card for retail purchase or cash advance. |
| **Remarks** | * A supplementary card can be activated even if the principal card is not yet active. * All processes in italicized font are done manually. |

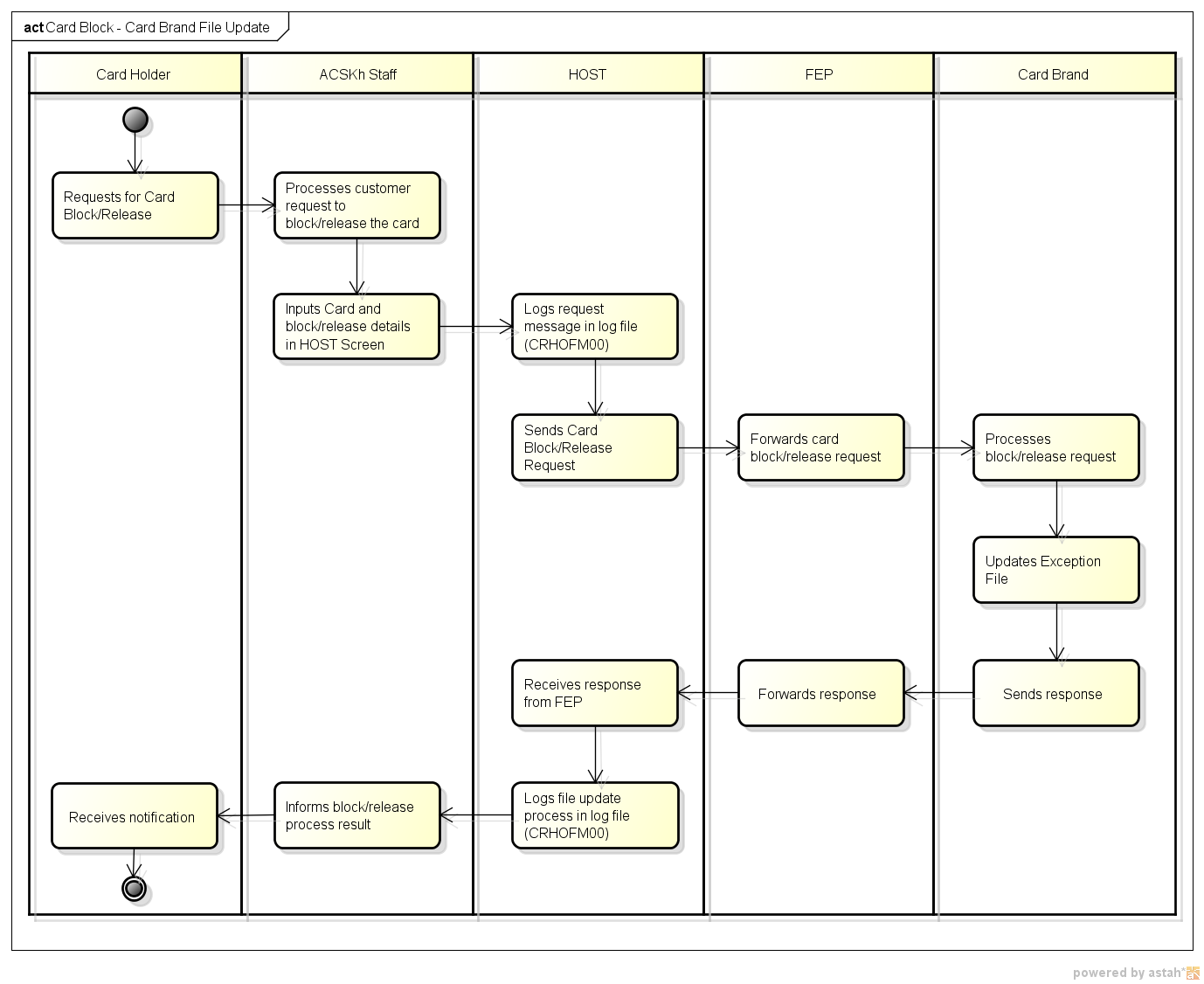
## FR004 Account Management

* 1. **FR004A Card Block – NEW FEP Block**

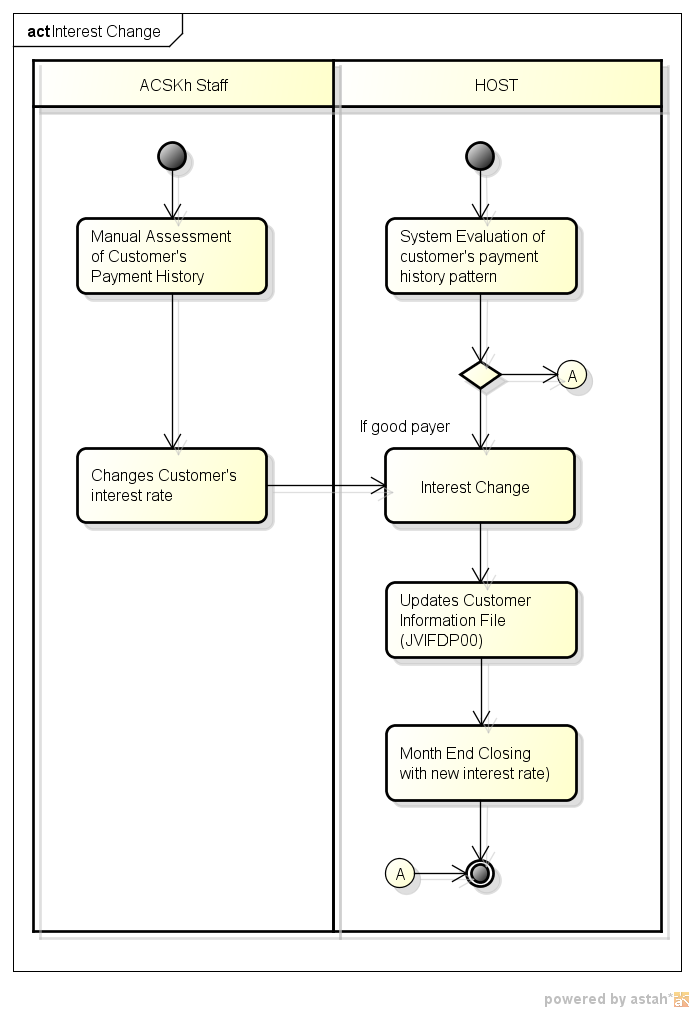


|  |  |
| --- | --- |
| Overview | NEW FEP Block function allows the user to block the card in HOST side and in NEW FEP side. By then, transactions that will go through NEW FEP will be automatically rejected; same goes with the transactions manually inputted in HOST screens. |
| Pre-condition | 1. Card was embossed. 2. Connection in TCP1 gateway is up. |
| Process | **Card Holder**   1. *Requests for card block/card release.*   **ACSKH Staff (Risk Management Department)**   1. *Processes customer’s card block/release request.* 2. *Inputs card and block details in HOST Screen*   **HOST**   1. Sends block request to NEW FEP   **NEW FEP Process**   1. Updates CARDTBL, sets the status to block. 2. Sends response to HOST   **HOST**   1. Receives response from NEW FEP 2. Updates Customer Information File’s Hold Code Field 3. Logs transaction to log file   **ACSKH Staff (Risk Management Department)**   1. *Informs block/release process result*   **Card Holder**   1. *Receives notification* |
| Result | Card was blocked and cannot do cash advance and credit purchase. |
| Remarks/Note | * Card blocking can also be done automatically once customer was delinquent. Different type of delinquencies corresponds to different type of block codes. Some block codes allows credit purchase but not the cash advance transactions. * All processes in *italicized font* are done manually. |

* 1. **FR004B Card Block – Card Brand File Update**

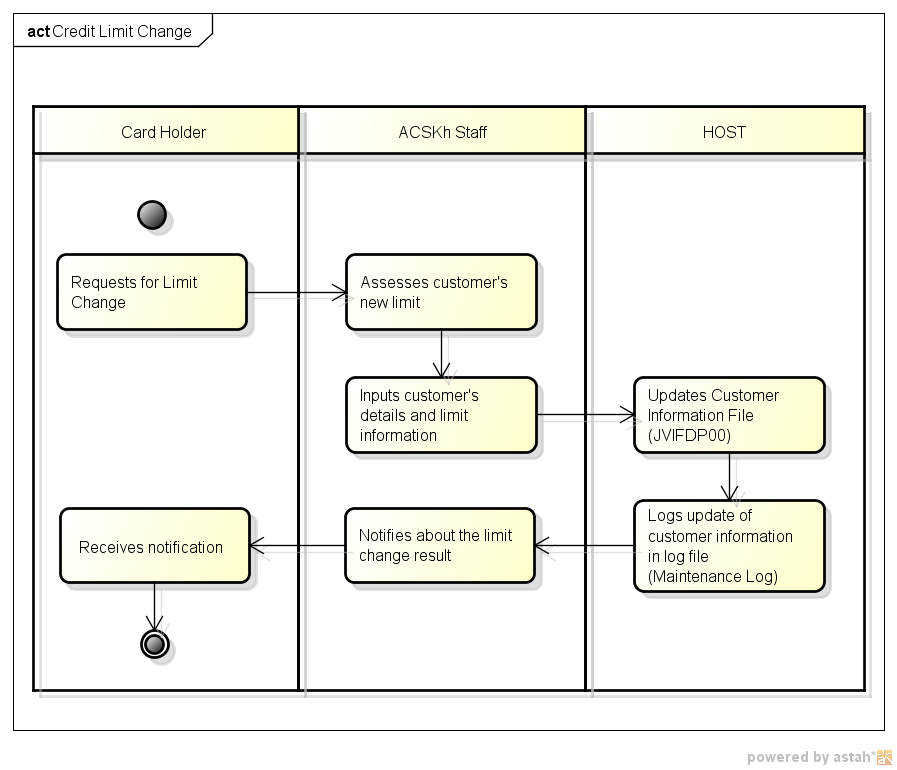


|  |  |
| --- | --- |
| Overview | Card Brand File Update allows the user to be block in Card Brand side. This will prevent the card holder to do transactions when Brand Stand-In. |
| Pre-condition | 1. Card was embossed. 2. Connection in TCP2 gateway is up. |
| Process | **Card Holder**   1. *Requests for card block/release.*   **ACSKH Staff (Risk Management Department)**   1. *Processes customer’s card block request.* 2. *Inputs card and block/release details in HOST Screen*   **HOST**   1. Sends block/release request to NEW FEP   **NEW FEP Process**   1. Forwards the block request to Card Brand   **Card Brand**   1. Processes block/release request 2. Updates Exception File 3. Sends response to NEW FEP   **NEW FEP Process**   1. Forwards response of Card Brand Network to HOST   **HOST**   1. Receives response from NEW FEP 2. Updates Customer Information File’s Hold Code Field 3. Logs transaction to log file   **ACSKH Staff (Risk Management Department)**   1. Informs block/release process result.   **Card Holder**   1. Receives notification |
| Result | Card was blocked and cannot do cash advance. |
| Remarks/Note | * When all requirements are completed and verified, the information will serve as input in the Data Application Entry * All processes in *italicized font* are done manually. |

* 1. **FR004C Interest Change**

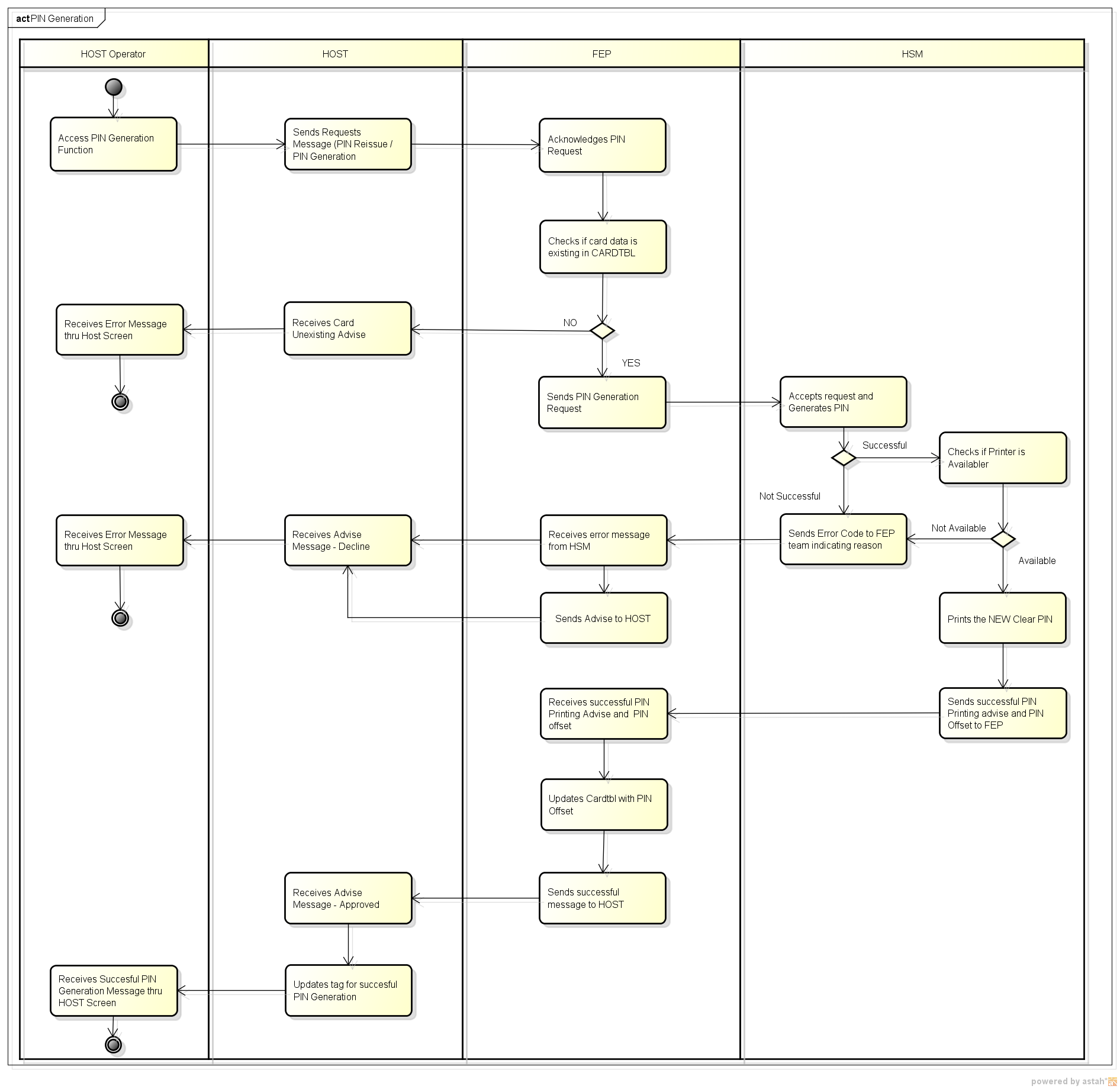
|  |  |
| --- | --- |
| Overview | Interest change comes in two processes. First is the manual change of interest rate group using HOST screen. Second is system’s automatic change of interest rate based on assessment on customer’s payment history. |
| Pre-condition | Automatic Process:   1. Customer is active customer for one year. |
| Process | Manual Interest Change:  **ACSKH Staff**   1. *Assesses customer’s payment history, if customer is a good payer* 2. *Changes customer’s interest rate using HOST Screen*.   **HOST**   1. Updates customer’s interest rate 2. In month end closing, interest rate that will be used is the new interest rate.   Automatic Interest Change:  **HOST**   1. Assesses customer payment history pattern 2. If customer is a good payer, changes interest rate to the next lower rate. 3. In month end closing, interest rate that will be used is the new interest rate. |
| Result | Customer’s interest rate will be changed. |
| Remarks/Note | All processes in *italicized* font are done manually. |

* 1. **FR004D Credit Limit Change**



|  |  |
| --- | --- |
| Overview | Credit Limit change function allows the user to change customer’s credit limit (limit down or limit up, permanent or temporary). |
| Pre-condition | Card must be activated. |
| Process | **Card Holder**   1. *Requests for credit limit change*   **ACSKH Staff**   1. *Assesses customer’s request to approve limit change* 2. *Inputs customer’s details and limit information*   **HOST**   1. Updates customer’s limit 2. Logs transaction to log file   **ACSKH Staff**   1. *Notifies staff about limit change request result*   **Card Holder**   1. *Receives notification* |
| Result | Customer’s credit limit will be changed. |
| Remarks/Note | All processes in *italicized font* are done manually. |

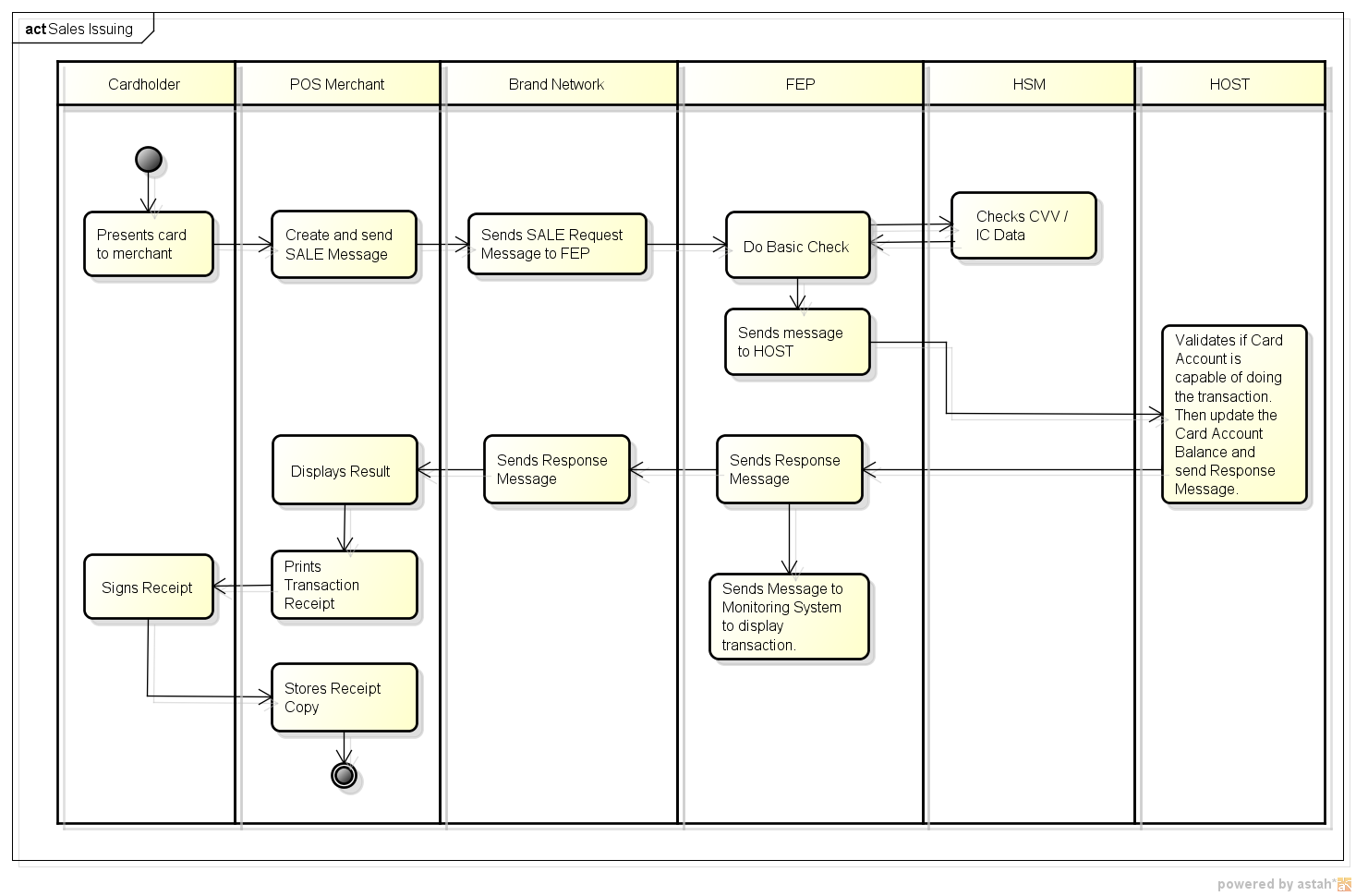
## FR005 PIN Generation Process



|  |  |
| --- | --- |
| **Overview** | This is the process of generating and printing random PIN to be sent to cardholder. PIN is necessary for Cash Advance Transaction. |
| **Pre-condition** | * Card number should be existing in HOST and NEW FEP database. * Established subsystem connection between HOST and NEW FEP. * Card was embossed. * PIN generation shall be user-triggered. |
| **Process** | **HOST**   1. In PIN Generation process, HOST will send PIN reissue / generation requests to NEW FEP.   **NEW FEP**   1. NEW FEP will then validate if the HOST requests if valid or not. 2. If valid, NEW FEP will send three PIN generation requests to HSM for the following: 3. Generates Encrypted PIN 4. Generates PIN Offset 5. Prints PIN 6. If not valid, NEW FEP will send Card Not Existing advise to HOST.   **HSM**   1. Generates the PIN for each request and will also print the PIN letter. 2. If PIN Printing is successful, HSM will complete the following tasks: 3. Prints the new CLEAR PIN 4. Sends successful PIN Printing advise and PIN Offset to NEW FEP 5. If PIN Printing is not successful, HSM notifies NEW FEP that PIN generation was successful or not to NEW FEP.   **NEW FEP**   1. If NEW FEP receives successful message, 2. Updates NEW FEP database using the Offset. 3. Sends successful message to HOST 4. If NEW FEP receives unsuccessful message, sends message to HOST.   **HOST**   1. If HOST receives successful message, Updates tag for successful PIN. |
| **Result** | * Approved – Successful Printing and generating of encrypted PIN and PIN Offset. * Declined – Unsuccessful PIN Generation |
| **Remarks** | Unsuccessful PIN generation requests will be processed on the next schedule.  PIN Printing is not included in the Process Flow; this would have to be decided by the client. |

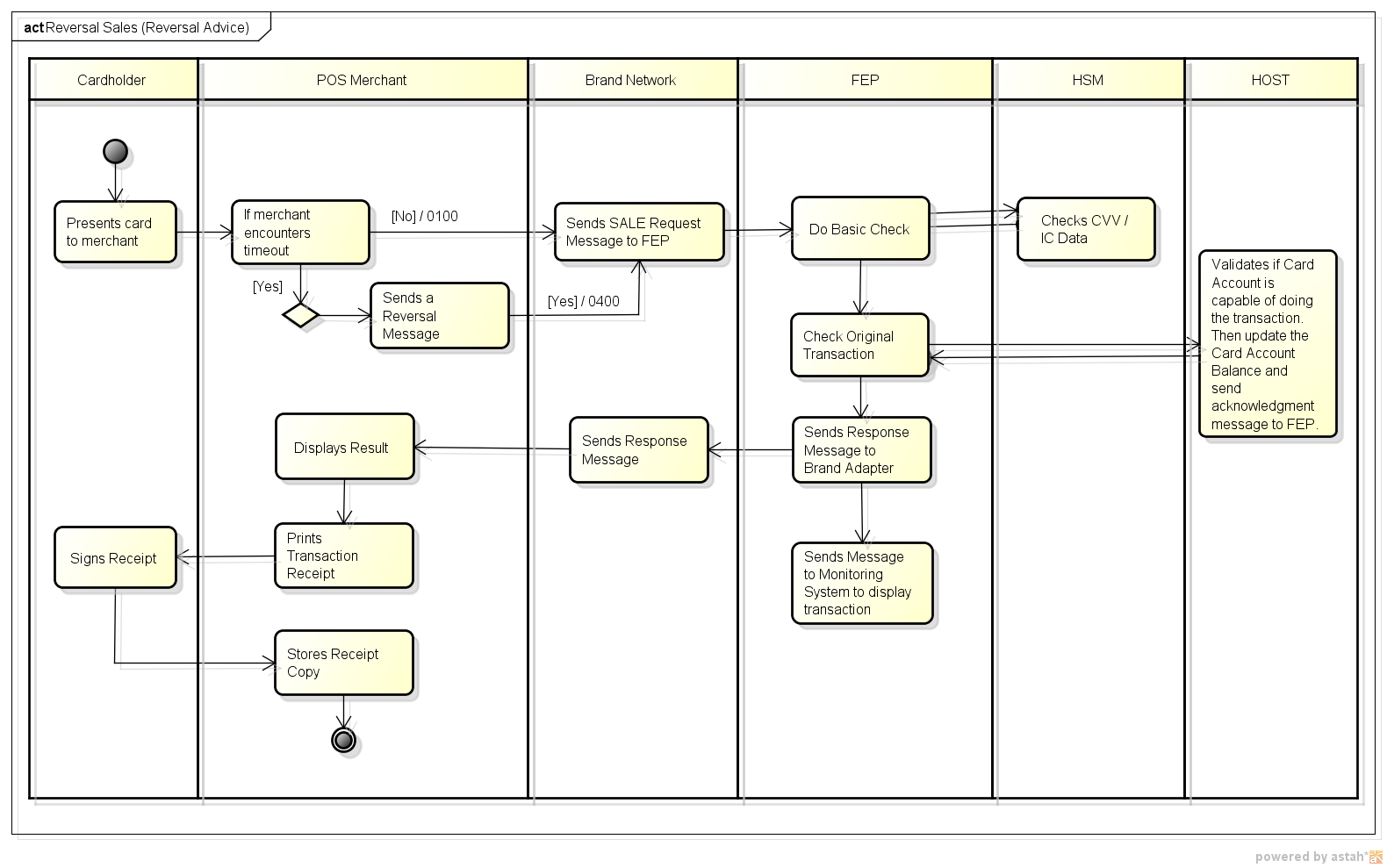
## FR006 Cards Transactions

* 1. **FR006A Sales Issuing**



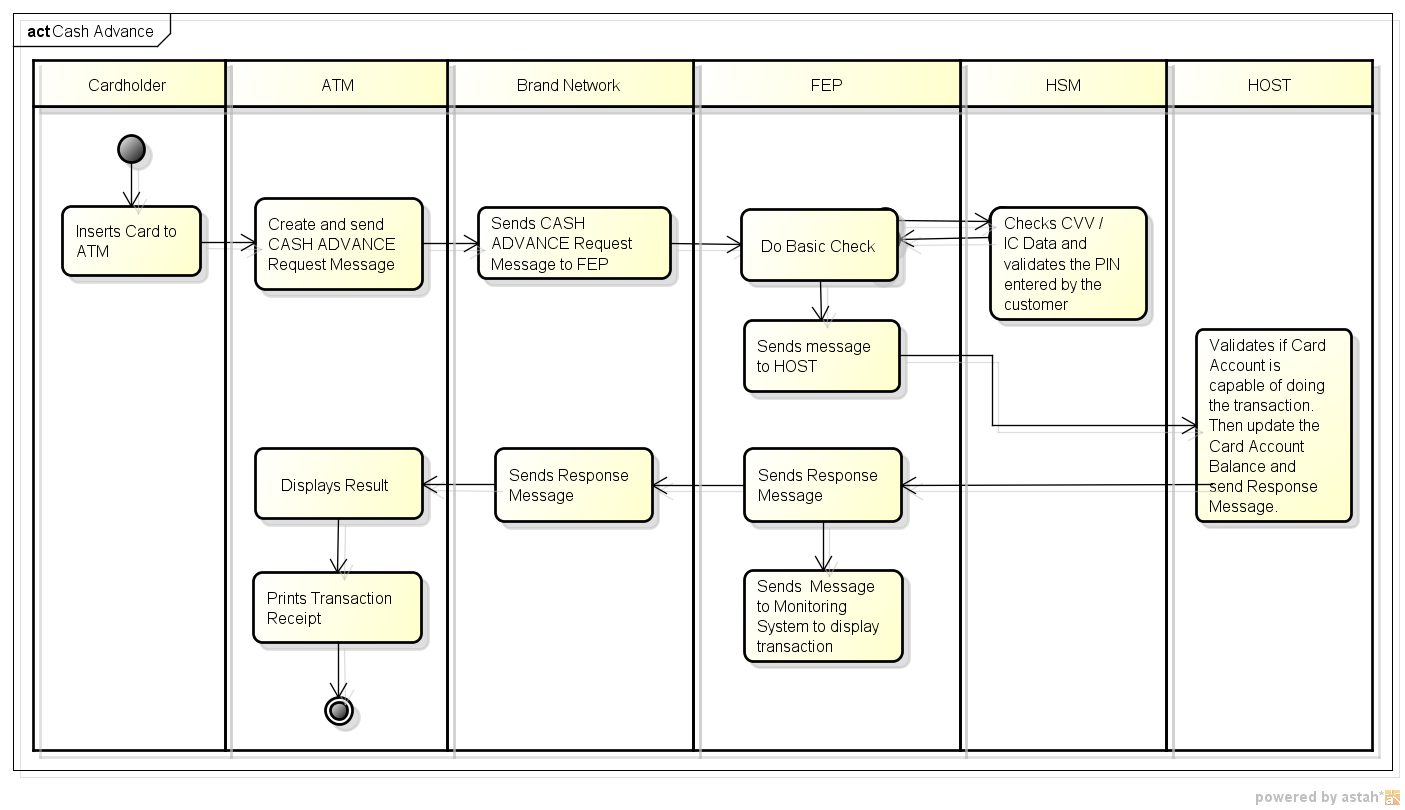
|  |  |
| --- | --- |
| **Overview** | Merchant performs Sales transaction via Non-AEON POS/EDC. |
| **Pre-condition** | 1. Transaction on POS/EDC with card using IC chip (insert), magnetic stripe (swipe entry) or manual entry.  2. Cardholder presents AEON card to purchase items.  3. Merchant uses the AEON card on the Non-AEON POS/EDC Terminal.  4. POS/EDC Terminal sends the transaction to the Acquiring Institution then the Acquiring Institution will forward this to Card Brand Network (VISA/MasterCard).  5. Card Brand Network will forward the transaction to NEW FEP.  6. After receiving the request message, NEW FEP will process the message. |
| **Process** | **REQUEST**  **Brand Network**   1. Sends sales message to NEW FEP (Brand Adapter).   **New FEP**  *Brand Adapter*   1. Sends Request message to NEW FEP Process for format checking (before sending to HOST).   *NEW FEP Process*   1. NEW FEP performs basic checking and sends CVV/iCVV/CVV2 to HSM for verification. 2. HSM sends response message to NEW FEP. 3. Sends request message to HOST adapter.   *HOST Adapter*   1. Create and sends HOST message format to HOST.   **HOST**   1. Validates transaction details including available limit. 2. Creates RAW transaction data in order to be matched during Settlement. 3. Updates the balance of the customer. 4. Sends response message back to HOST Adapter.   **RESPONSE**  **New FEP**  *HOST Adapter*   1. Sends response message back to NEW FEP Process.   *NEW FEP Process*   1. Sends response message back to Brand Adapter.   *Brand Adapter*   1. Forwards response message to Brand Network. 2. Sends transaction to Monitoring System via MON SAF in order for the transaction to be displayed in the Monitoring Screen. |
| **Stand In Process** | If HOST encounters Timeout or HOST is unavailable, NEW FEP process will authorize transaction/s in behalf of HOST, following the Stand-In criteria. |
| **Result** | 1. Brand Network sends response back to POS.   1. If the transaction is approved,    1. Merchant prints the transaction receipt.    2. Cardholder signs the receipt.    3. Merchant stores the receipt copy. 2. If the transaction is declined, POS/EDC will display declined message on screen |
| **Remarks** | For Stand-In case, once HOST is already online, NEW FEP will send the advice data to HOST thru HOST SAF connection.  Monitoring System functions/processes are included in the NEW FEP system function. |

* 1. **FR006B Reversal Sales (Reversal Advice)**



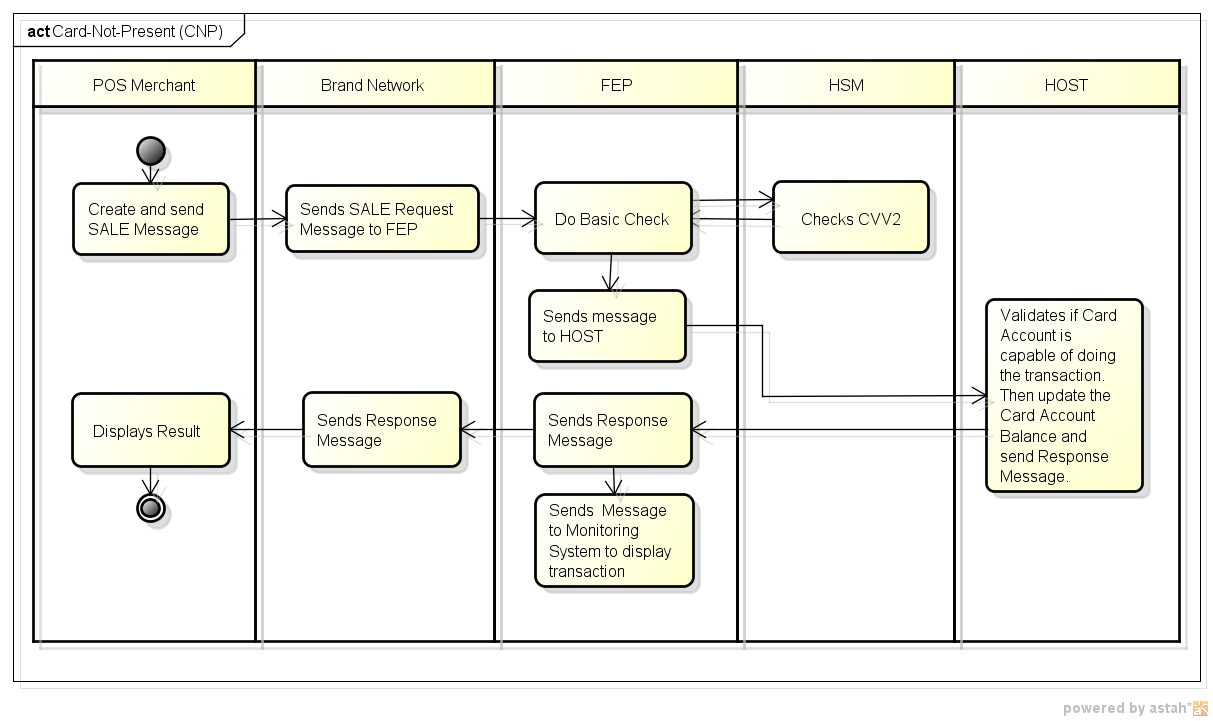
|  |  |
| --- | --- |
| **Overview** | Merchant performs Sales transaction but encountered timeout. |
| **Pre-condition** | Cardholder used AEON Card but suddenly encountered timeout and transaction was not completed. Possible reason of time out can be either of the following:  1. When Brand Network Timeout occurs, Brand Network needs to send the Reversal Message.  2. When POS/EDC Terminal timeout occurs, POS/EDC automatically sends a Reversal Message.  3. When POS/EDC Terminal sends Void Transaction. |
| **Process** | **REQUEST**  **Brand Network**   1. Sends reversal message to NEW FEP (Brand Adapter).   **New FEP**  *Brand Adapter*   1. Sends Request message to NEW FEP Process for format checking (before sending to HOST).   *NEW FEP Process*   1. Performs basic checking and sends CVV/iCVV/CVV2 to HSM for verification. 2. Checks for the original transaction. 3. If original transaction exists, 4. NEW FEP sends request message to HOST adapter and 5. NEW FEP sends response message to Brand Adapter.   *Brand Adapter*   1. Creates and sends response message format to Brand Network. 2. Sends transaction to Monitoring System via MON SAF in order for the transaction to be displayed in the Monitoring Screen.   *HOST Adapter*   1. Creates and sends HOST message format to HOST thru HOST SAF connection.   **HOST**   1. HOST checks for the original transaction. 2. Processes and updates the balance of the customer. 3. Sends acknowledgment message back to HOST Adapter. |
| **Stand-In Process** | Transaction is sent to HOST thru HOST SAF connection. |
| **Result** | The transaction is reversed. |
| **Remarks** | * Brand Network will send a reversal repeat message to HOST via NEW FEP if Brand Network does not receive reversal advice response from HOST. * If HOST receives a reversal request message, it should send a reversal response. * If during sending, the reply back to EDC and the connection encountered timeout, the EDC will send reversal request again but NEW FEP will just send approve response since it is already approve in the first request. * Monitoring System functions/processes are included in the NEW FEP system function. |

* 1. **FR006C Cash Advance**



|  |  |
| --- | --- |
| **Overview** | Customer performs Cash Advance transaction via Non-AEON ATM. |
| **Pre-condition** | 1. Enters Personal Identification Number on ATM numeric pad.  2. ATM sends the transaction to the Acquiring Institution then the Acquiring Institution will forward this to Card Brand Network (VISA/MasterCard).  3. Card Brand Network will forward the transaction to NEW FEP.  4. After receiving the request message, NEW FEP will process the message. |
| **Process** | **REQUEST**  **Brand Network**   1. Sends Cash Advance message to NEW FEP (Brand Adapter).   **New FEP**  *Brand Adapter*   1. Brand Adapter will send Request message to NEW FEP Process for format checking (before sending to HOST).   *NEW FEP Process*   1. NEW FEP performs basic checking and sends PIN Block to HSM for verification. 2. HSM returns PIN Offset value to NEW FEP. 3. NEW FEP validates PIN Offset received from HSM against the PIN Offset stored in the database. 4. Sends request message to HOST adapter.   *HOST Adapter*   1. Create and sends HOST message format to HOST for final authorization.   **HOST**   1. Validates transaction details including available limit. 2. Creates MATCH transaction data. 3. Updates the balance of the customer. 4. Sends response message back to HOST Adapter.   **RESPONSE**  **New FEP**  *HOST Adapter*   1. Sends response message back to NEW FEP Process.   *NEW FEP Process*   1. Sends response message back to Brand Adapter.   *Brand Adapter*   1. Forwards response message to Brand Network. 2. Sends transaction to Monitoring System via MON SAF in order for the transaction to be displayed in the Monitoring Screen. |
| **Stand In Process** | If there is HOST Timeout or HOST is unavailable, NEW FEP will automatically decline the transaction since cashing transaction is not supported during Stand-In. |
| **Result** | 1. Brand Network sends response back to ATM.  2. If the transaction is approved, ATM will print the transaction receipt and cash will disburse.  3. If the transaction is declined, ATM will display declined message on screen |
| **Remarks** | * If ATM encounters error during the transaction, the Acquirer sends a Reversal Message to the Brand Network. Brand Network will then forward the Reversal Message to the Issuer. * Monitoring System functions/processes are included in the NEW FEP system function. |

* 1. **FR006D Card Not Present (CNP) Transactions**



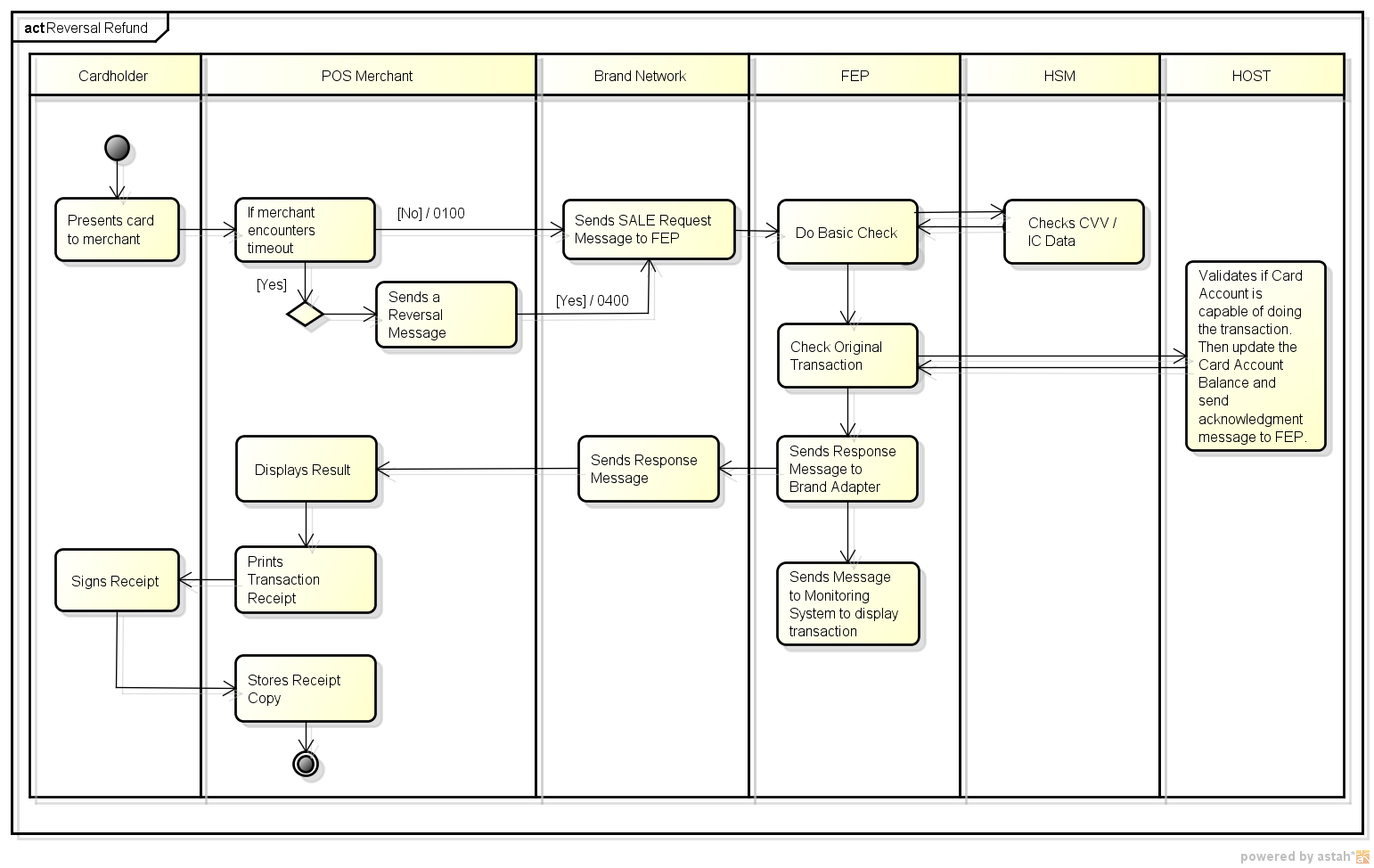
|  |  |
| --- | --- |
| **Overview** | Cardholder performs Card Not Present transactions (e.g. MOTO, E-commerce, and Recurring). |
| **Pre-condition** | The following scenarios fall under CNP transactions:  1. MOTO/Recurring – Cardholder provided the Card number and Expiration Date to the merchant.  2. E-Commerce – Cardholder provided the Card Number, Expiration Date and CVV2 via website. |
| **Process** | **REQUEST**  **Brand Network**   1. Sends Sale message to NEW FEP (Brand Adapter).   **New FEP**  *Brand Adapter*   1. Brand Adapter will send Request message to NEW FEP Process for format checking (before sending to HOST).   *NEW FEP Process*   1. NEW FEP performs basic checking and sends CVV2 to HSM for verification. 2. HSM sends response message to NEW FEP. 3. Sends request message to HOST adapter.   *HOST Adapter*   1. Create and sends HOST message format to HOST.   **HOST**   1. Validates transaction details including available limit. 2. Creates RAW transaction data in order to be matched during Settlement. 3. Updates the balance of the customer. 4. Sends response message back to HOST Adapter.   **RESPONSE**  **New FEP**  *HOST Adapter*   1. Sends response message back to NEW FEP Process.   *NEW FEP Process*   1. Sends response message back to Brand Adapter.   *Brand Adapter*   1. Forwards response message to Brand Network. 2. Sends transaction to Monitoring System via MON SAF in order for the transaction to be displayed in the Monitoring Screen. |
| **Stand In Process** | If there is HOST Timeout or HOST is unavailable, NEW FEP process will authorize the transaction in behalf of HOST by judging the amount. |
| **Result** | 1. Brand Network sends the response back to POS.  2. If the transaction is approved,  2.1. Merchant prints the transaction receipt.  2.2 Cardholder signs the receipt.  2.3 Merchant stores the receipt copy.  3. If the transaction is declined, POS/EDC will display declined message on screen |
| **Remarks** | * For Stand-In case, once HOST is already online, NEW FEP will send the advice data to HOST thru HOST SAF connection. * CVV2 may not be present for Recurring Transactions. |

* 1. **FR007E Refund (Issuing)**



|  |  |
| --- | --- |
| ***Overview*** | Successfully completed sales transaction and settlement’s already done; or customer wants to return the products. |
| ***Pre-condition*** | 1. Cardholder has completed successful **Sale** transaction with the merchant using Non-AEON EDC terminal. 2. Cardholder presents the transaction receipt to the merchant. 3. Merchant enters the information needed for refund transaction in a Non-AEON EDC terminal. 4. Cashier select refund and enter amount to be refunded 5. Sends EDC message to Brand Network. 6. From Brand Network, request message will be forwarded to NEW FEP. |
| ***Process*** | **REQUEST**  **New FEP**  *Brand Network*   1. Sends Refund Request message to NEW FEP (Brand Adapter).   *Brand Adapter*   1. Brand Adapter will send Request message to NEW FEP for format checking.   *NEW FEP Process*   1. NEW FEP performs basic checking and sends CVV2 to HSM for verification. 2. HSM sends response message to NEW FEP. 3. Sends request message to HOST adapter.   *HOST Adapter*   1. Create and sends HOST message format to HOST.   **HOST**   1. Validates transaction details including available limit. 2. Creates RAW transaction data in order to be matched during Settlement. 3. Updates the balance of the customer. 4. Sends response message back to HOST Adapter.   **RESPONSE**  **New FEP**  *HOST Adapter*   1. Sends response message back to NEW FEP Process.   *NEW FEP Process*   1. Sends response message back to Brand Adapter.   *Brand Adapter*   1. Forwards response message to Brand Network. 2. Sends transaction to Monitoring System via MON SAF in order for the transaction to be displayed in the Monitoring Screen. |
| ***Stand-in Process*** | If HOST Timeouts or HOST is unavailable, NEW FEP process will authorize the transaction in behalf of HOST by judging the amount. |
| ***Result*** | 1. If the transaction is approved,    1. Merchant prints the transaction receipt.    2. Cardholder signs the receipt.    3. Merchant stores the receipt copy. 2. If the transaction is rejected, EDC will display reject message on screen |
| ***Remarks*** | * To cancel refund transaction before settlement, the **Void Refund** transaction is performed. * If the refund transaction encounters timeout, the **Reversal Refund** Transaction is sent by EDC Terminal. |

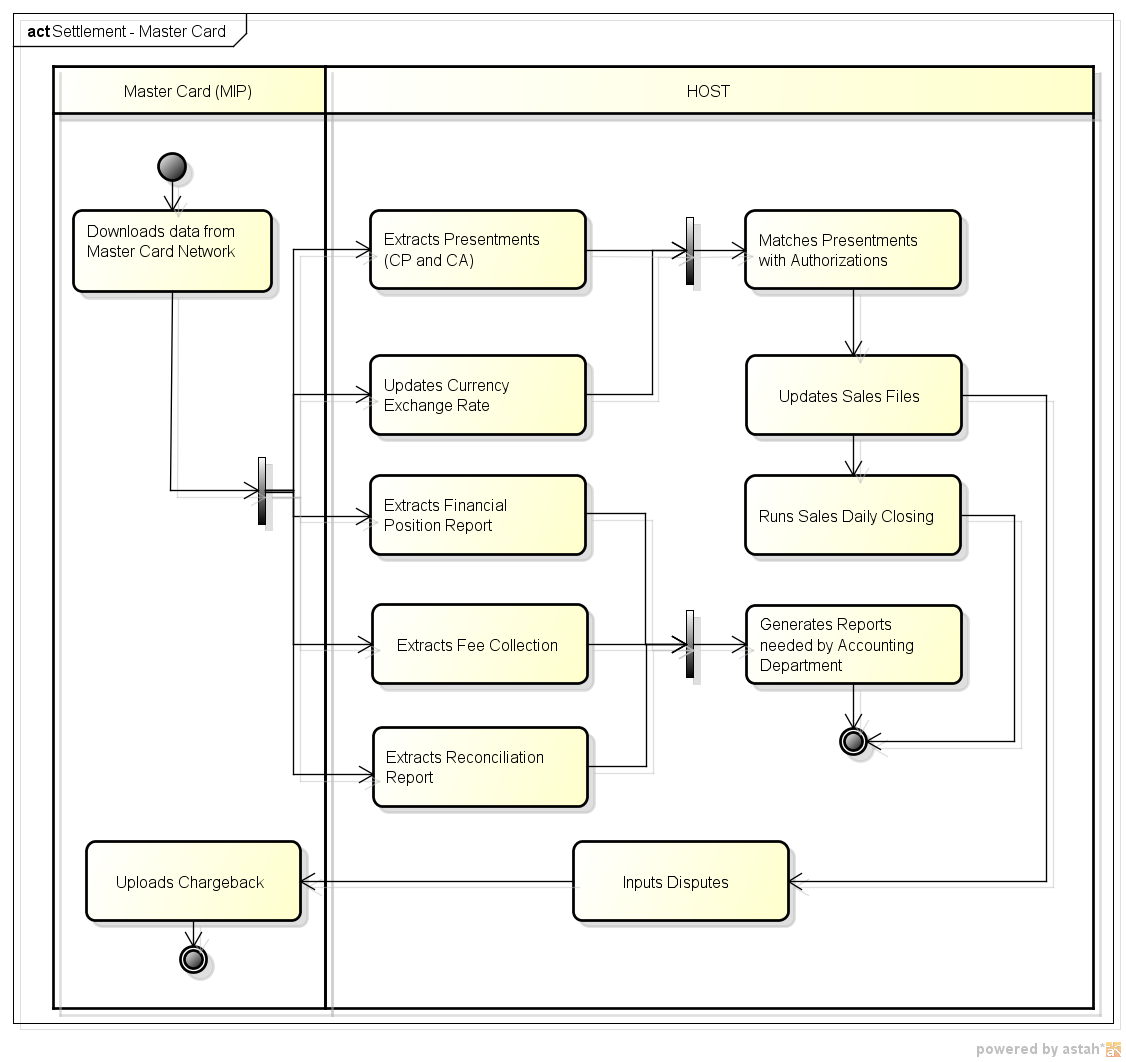
* 1. **FR006F Reversal Refund**



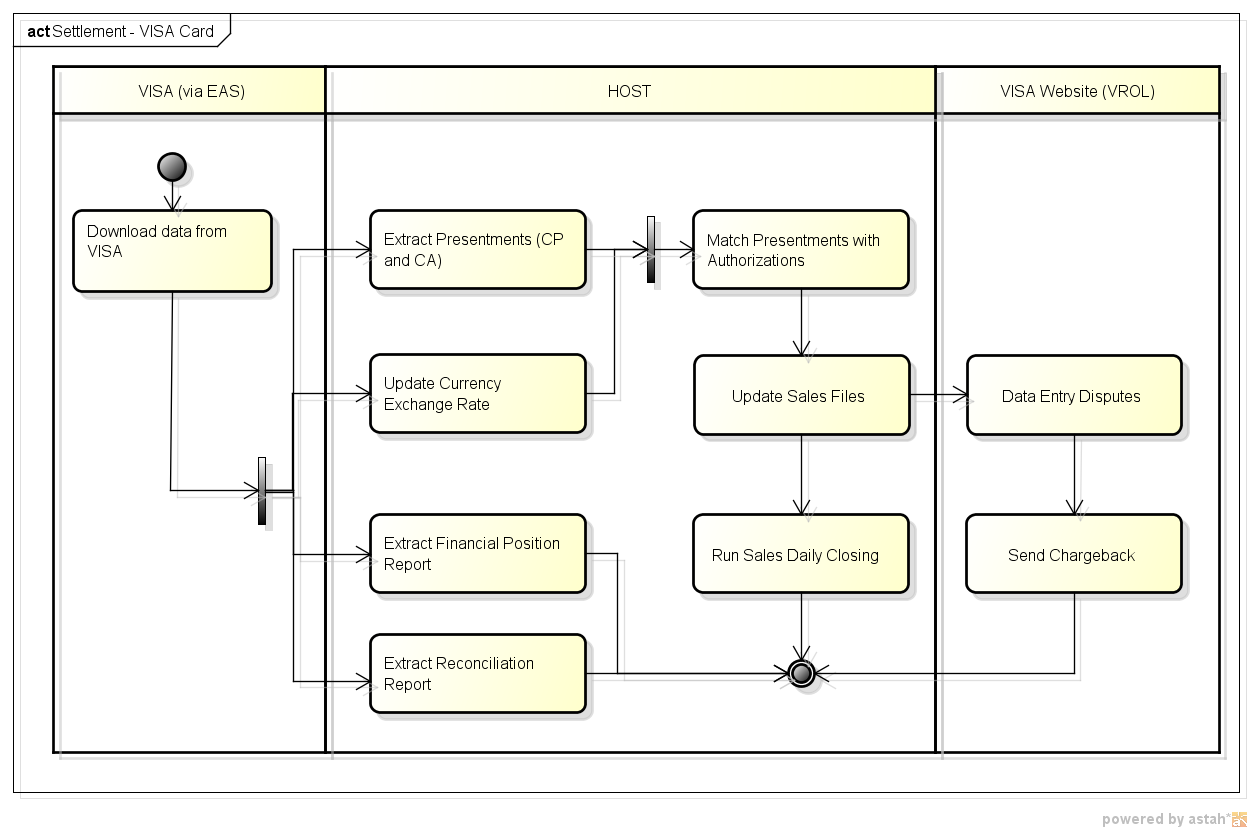
|  |  |
| --- | --- |
| ***Overview*** | Merchant transact Refund transaction but EDC encountered timeout. |
| ***Pre-condition*** | 1. Cardholder has completed successful **Sale** transaction with the merchant using Non-AEON EDC terminal. 2. Merchant process the **Refund** transaction but EDC terminal encountered timeout. |
| ***Process*** | **REQUEST**  **EDC Terminal**   1. Sends reversal message to EDC Adapter.   **Brand Network**   1. Sends reversal message to NEW FEP (Brand Adapter).   **New FEP**  *Brand Adapter*   1. Brand Adapter will send Request message to NEW FEP Process for format checking (before sending to HOST).   *NEW FEP Process*   1. NEW FEP performs basic checking and sends CVV/iCVV/CVV2 to HSM for verification. 2. NEW FEP checks for the original transaction. 3. If original transaction exists, 4. NEW FEP sends request message to HOST adapter and 5. NEW FEP sends response message to Brand Adapter.   *Brand Adapter*   1. Creates and sends response message format to Brand Network. 2. Sends transaction to Monitoring System via MON SAF in order for the transaction to be displayed in the Monitoring Screen.   *HOST Adapter*   1. Creates and sends HOST message format to HOST thru HOST SAF connection.   **HOST**   1. HOST checks for the original transaction. 2. Process and update the balance of the customer. 3. Sends acknowledgment message back to HOST Adapter. |
| ***Stand-In Process*** | Transaction is sent to HOST thru HOST SAF connection. |
| ***Result*** | The transaction is reversed. |
| ***Remarks*** | * Brand Network will send a reversal repeat message to HOST via NEW FEP if Brand Network does not receive reversal advice response from HOST. * If HOST receive a reversal request message, it should send a reversal advice response. * If during sending, the reply back to EDC and the connection encountered timeout, the EDC will send reversal request again but NEW FEP will just send approve response since it is already approve in the first request. |

## FR007 Settlement Process

1. **FR007A MasterCard Settlement**

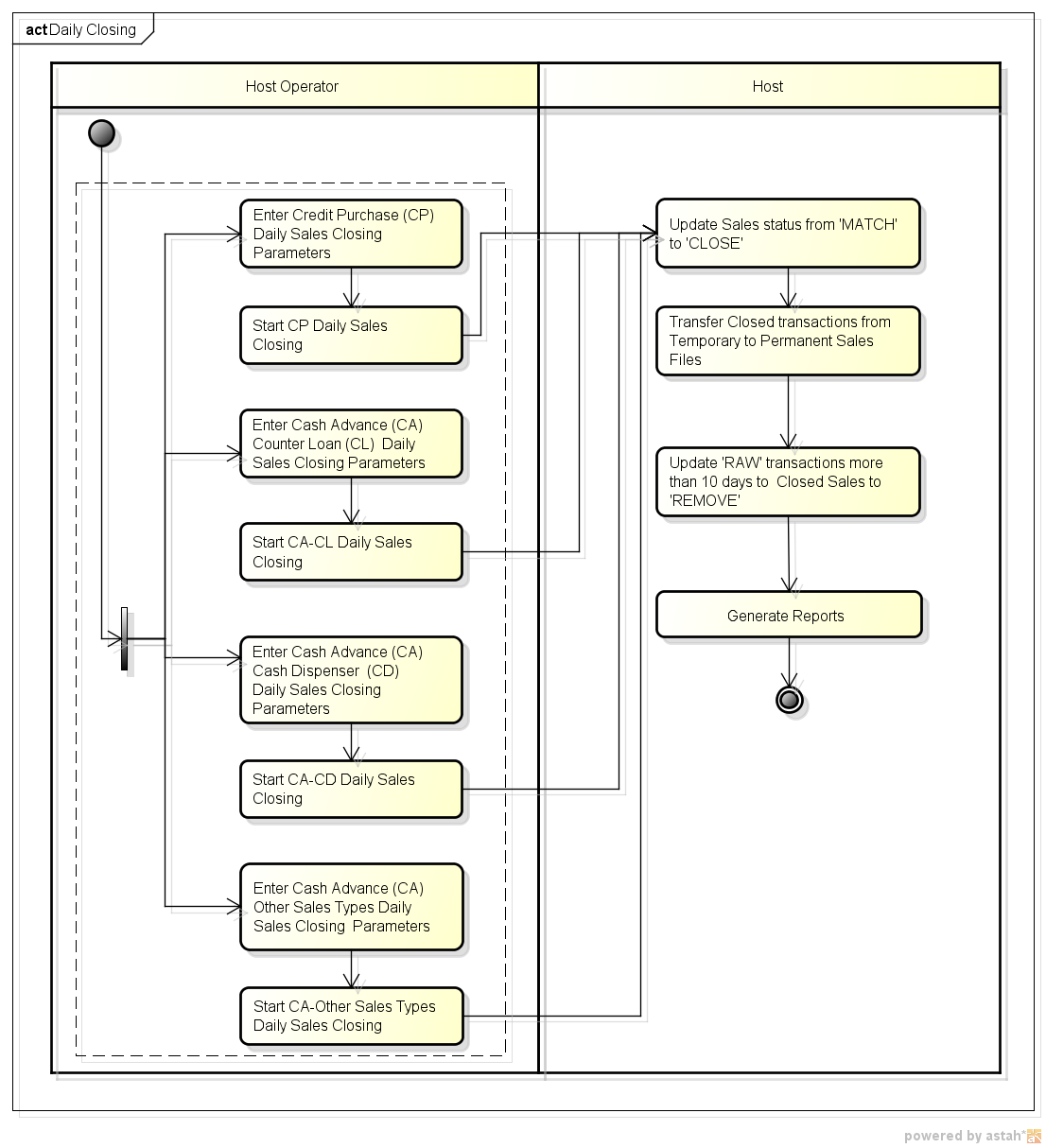


|  |  |
| --- | --- |
| **Overview** | Incoming Settlement from MasterCard are picked-up from MasterCard Interface Processor (MIP) via File Transfer Protocol (FTP) by the HOST. The settlement file is split into Presentment, Financial Position Report, Fee Collection, Currency Exchange Rate, and Reconciliation Report. The Presentment, being records of financial transactions, proceed into Sales Matching process with authorization transactions in the Temporary Sales File. Matched transactions are updated as ‘MATCH’ from ‘RAW’ while unmatched Presentment records are forced-match with status ‘MATCH’. These records are required for the Daily Sales Closing.  Presentment Report Summary, Financial Position Reports, Fee Collection, Currency Exchange Rate, and Reconciliation Reports are referred to by Finance Department. |
| **Pre-condition** | 1. Approved authorizations from Acquirers to Issuers that are with status ‘RAW’. 2. Settlement File should already be available in the MIP. |
| **Process** | **HOST**  Based on the downloaded data from the MasterCard Network:   1. Extracts Presentments (CP and CA). 2. Updates Currency Exchange Rate.    1. Upon completion of processes 1-2, HOST matches the Presentments with Authorizations.    2. Host updates sales files and then updates disputes files (should there be any) by conducting the Matching process. All FORCED MATCH will be processed in the system.    3. Host runs Sales Daily Closing. 3. Extracts Financial Position Report. 4. Extracts Fee Collection. 5. Extracts Reconciliation report.    1. Upon completion of processes 3-5, HOST generates reports needed by Accounting Department. |
| **Stand-In Process** | Not applicable. |
| **Result** | Sales transactions with ‘MATCH’ statuses. |
| **Remarks** | Sales transactions are now ready for Daily Sales Closing. |

1. **FR007B VISA Settlement**

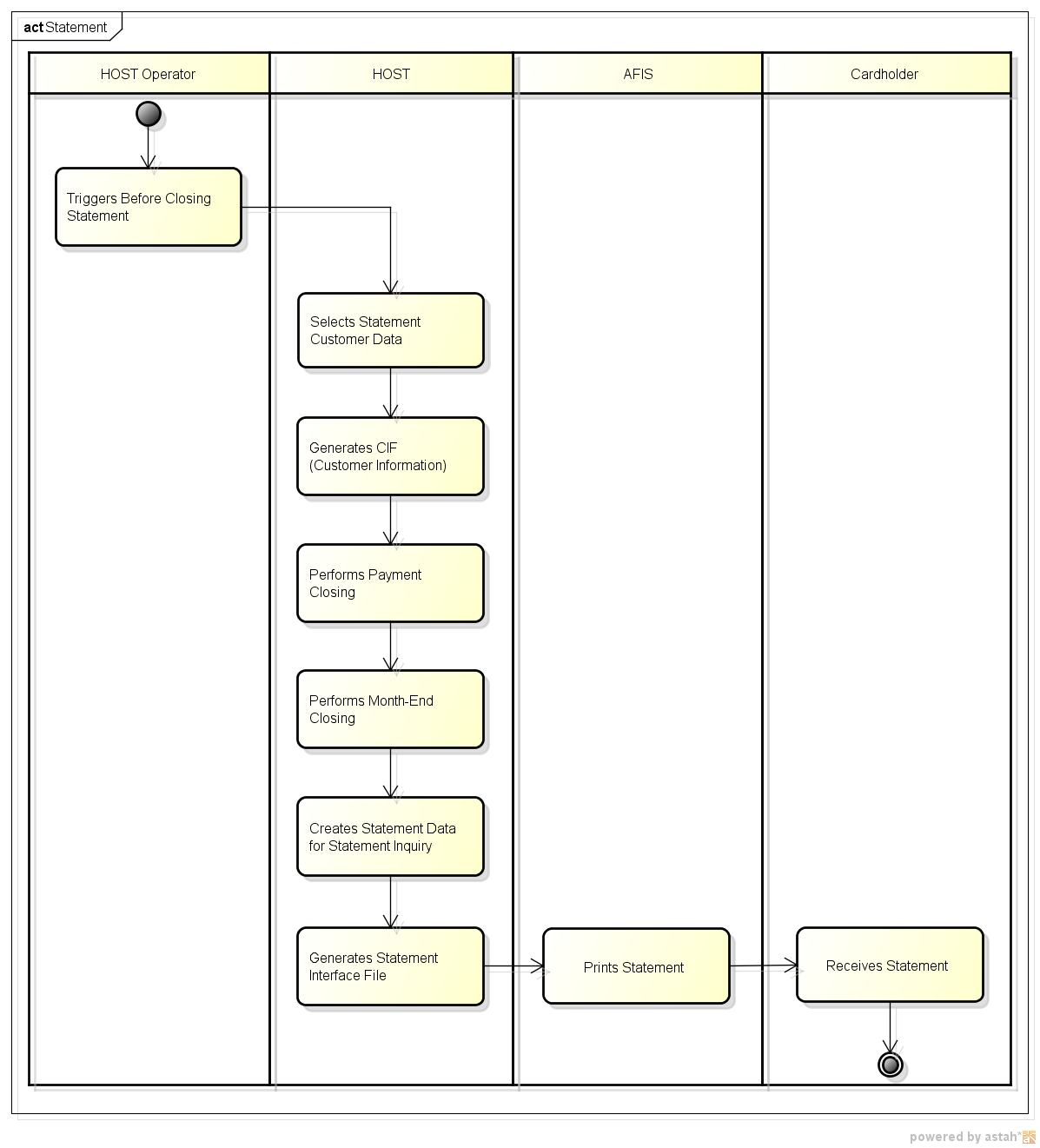
|  |  |
| --- | --- |
| **Overview** | Incoming Settlement from VISA are picked-up from EA Server via VISA Edit Package. The settlement file is split into Presentment, Financial Position Reports, Currency Exchange Rate, and Reconciliation Reports. The Presentment, being records of financial transactions, proceed into Sales Matching process with authorization transactions in the Temporary Sales File. Matched transactions are updated as ‘MATCH’ from ‘RAW’ while unmatched Presentment records are forced-match with status ‘MATCH’. These records are required for the Daily Sales Closing.  Presentment Report Summary, Financial Position Reports, Currency Exchange Rate, and Reconciliation Reports are referred to by Finance Department. |
| **Pre-condition** | * Approved authorizations from Acquirers to Issuers that are with status ‘RAW’. * Settlement File should already be in the EA Server. * Edit Package should be installed and connected to the EA Server. * Edit Package downloaded the Settlement File in EA Server. |
| **Process** | **HOST**  Based on the downloaded data from the VISA Network:   1. Extracts Presentments (CP and CA). 2. Updates Currency Exchange Rate.    1. Upon completion of processes 1-2, HOST matches the Presentments with Authorizations.    2. Host updates sales files. The VISA website (VROL) can also be used to charge back disputed transactions.    3. Host runs Sales Daily Closing. 3. Extracts Financial Position Report. 4. Extracts Reconciliation report. |
| **Stand-In Process** | Not applicable. |
| **Result** | Sales transactions with ‘MATCH’ statuses. |
| **Remarks** | Sales transactions are now ready for Daily Sales Closing. |

## FR008 Daily Sales Closing Process



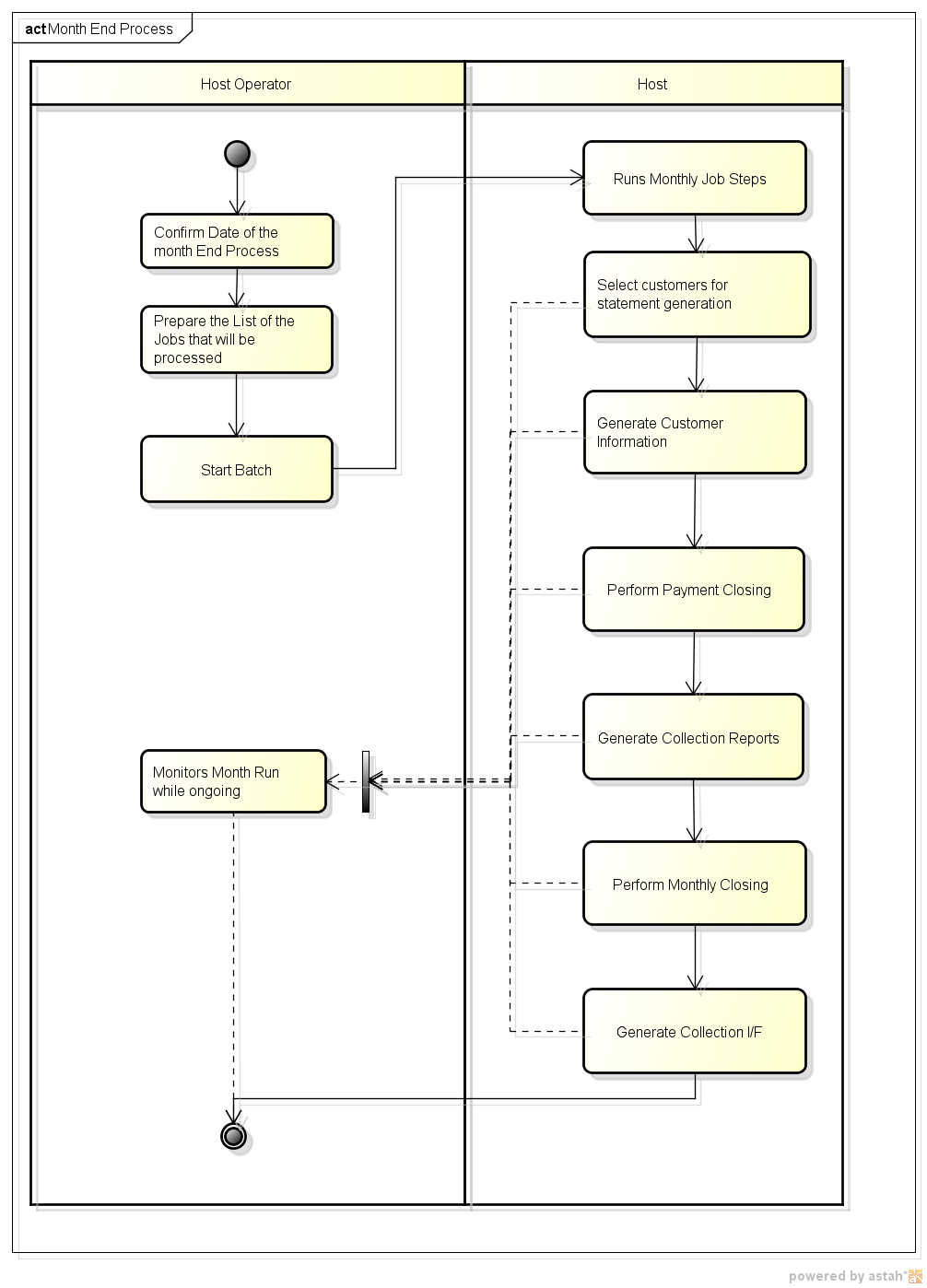
|  |  |
| --- | --- |
| **Overview** | Daily Sales Closing covers the Sales Period for the day. |
| **Pre-condition** | Prior to Daily Closing, the following process should be completed:   * VISA Settlement/Card Matching * MasterCard Settlement/Card Matching   For Credit Purchase Closing, the following information are needed:   * Business Code (e.g. VS,MC) * Agency/Merchant Code * Closing Date   For Cash Advance/Handling Charges Closing, the following information are needed:   * Business Code * Sales Type * Closing Date |
| **Process** | **HOST Operator**   1. Enters Credit Purchase (CP) Daily Sales Closing Parameters, then starts CP Daily Sales Closing 2. Enters Cash Advance (CA) Counter Loan (CL) Daily Sales Closing Parameters, then starts CA-CL Daily Sales Closing 3. Enters Cash Advance (CA) Cash Dispenser (CD) Daily Sales Closing Parameters, then starts CA-CD Daily Sales Closing 4. Enters Cash Advance (CA) Other Sales Types Daily Sales Closing Parameters, then starts CA- Other Sales Types Daily Sales Closing   **HOST**   1. Updates Sales status from 'MATCH' to 'CLOSE' 2. Transfers Closed transactions from Temporary to Permanent Sales Files 3. Updates 'RAW' transactions without settlement for more than 10 days to have a Status of 'REMOVE' 4. Generates Reports |
| **Stand-In Process** | Not Applicable. |
| **Result** | 1. The following Reports will be generated:    1. Settlement List Detail Report    2. Settlement List Summary Report    3. Daily Sales Checklist Report    4. Sales Remove Report 2. Possible Sales Status after Daily Closing:  * CLOSED - Sales Transactions that were previously "MATCH". * REMOVE - Sales Transactions without Settlement File for more than 10 Days. * DELETE - Sales Transactions with status "RAW" that have been reversed. |
| **Remarks** | This module can be done daily or depending on the client's preference considering the Sales Period covered. |

## FR009 Statement Process



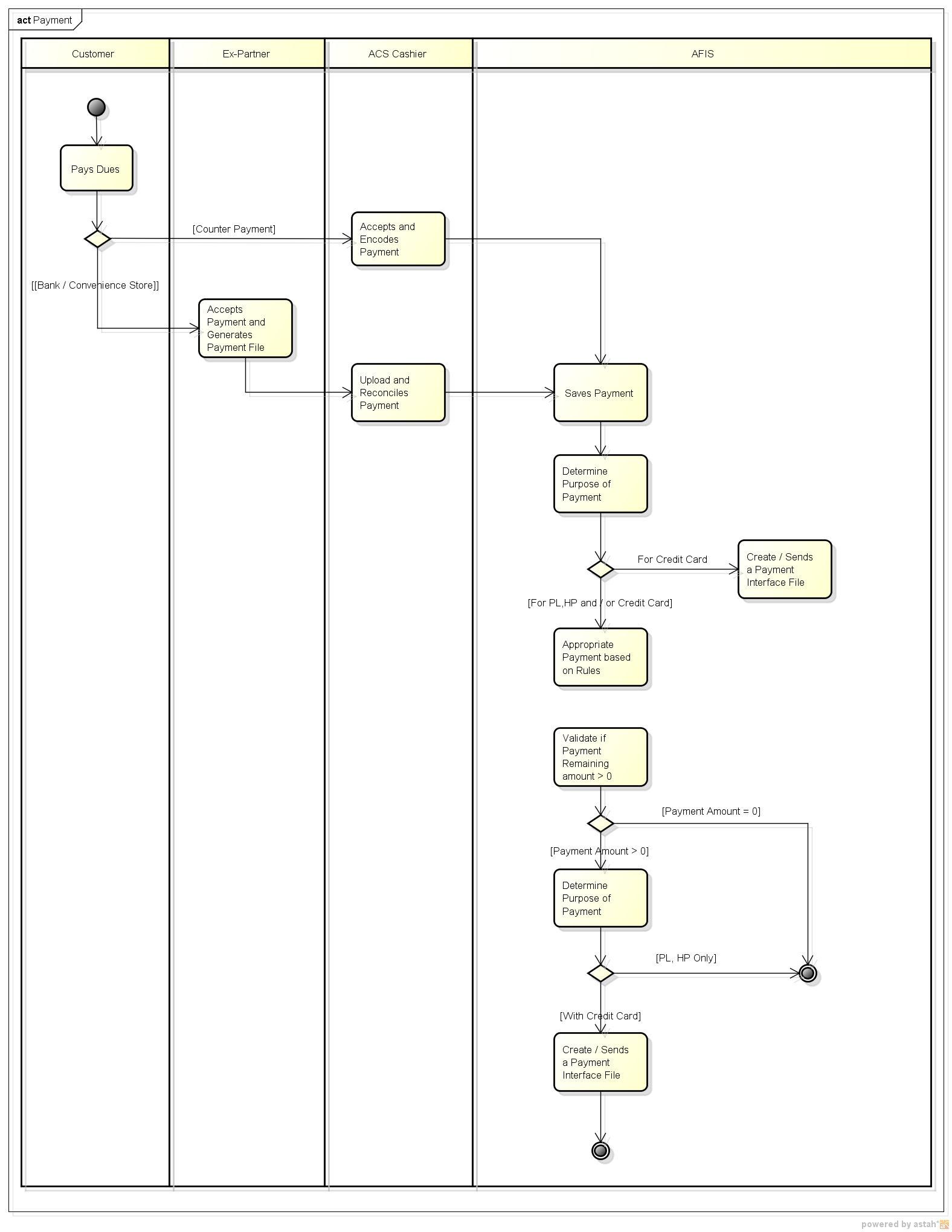
|  |  |
| --- | --- |
| **Overview** | System allows for generation of Statement before End of Month Process. This can be on the 11th, 13th, and 16th for the final statement.  Closed sales transactions from the 11th of the previous month to the 10th of the current month are included.  Payment transactions made from the 21st of the previous month to the current date up to the Monthly Closing are included.  Interests are calculated based on allocation of payment received.  The previous balance brought forward and the new balance is calculated. |
| **Pre-condition** | * Prior Point Calculation run. * Prior Membership Fee Generation run. * If there are any remaining sales transactions with ‘MATCH’ status, Daily Sales Closing needs to be executed. * Statement is printed for all new cards on the 11th. * Statement is printed if the Total billing amount is greater than the predefined amount by the Issuer. * Statement is printed if a Payment was made for a previous balance and is greater than the predefined amount by the Issuer. |
| **Process** | **HOST Operator**   1. Triggers Before Closing Statement   **HOST**   1. Selects Statement Customer Data 2. Generates CIF (Customer Information) 3. Performs Payment Closing 4. Performs Month-End Closing 5. Creates Statement Data, which the Customer Service Staff can inquire 6. Generates Statement Interface File   **AFIS**   1. Prints Statement 2. Sends Statement to Cardholder |
| **Stand-In Process** | Not applicable. |
| **Result** | 1. Statements are combined for principal and supplementary cards. Transactions are grouped by card number. The principal’s mailing address serves as the delivery address. 2. Customer service can view online previous statements (not the exact replica of the statement on paper). Customer service can also initiate customer re-print upon customer request. |
| **Remarks** | * Predefined amounts for printing statements should be set by the Issuer prior to launching the business. * Customers with total billing greater than the predefined amount set by the Issuer (e.g. 10 USD) with payments at least equal to the Minimum Payment made from the 21st of the previous month until the 10th of current month will have their statements printed on the 11th. * Customers with total billing greater than the predefined amount set by the Issuer with payments at least equal to the Minimum Payment made from the 11th to the 12th of current month will have their statements printed on the 13th. * Customers with total billing greater than the predefined amount set by the Issuer with payments at least equal to the Minimum Payment made from the 13th  to the 15th of current month will have their statements printed on the 16th * Customers with total billing greater than the predefined amount set by the Issuer with payments at least equal to the Minimum Payment made from the 16th to the 20th of current month will have their statements generated, but not printed on the 21st. * Customers with **total billing greater than the predefined amount set by the Issuer** but **did not make any payments** will have their statements generated, but not printed on the21st. |

## FR010 End of Month Process



|  |  |
| --- | --- |
| **Overview** | This process back-ups necessary files for recovering purposes before and after month end and payment closing, monthly statement, monthly collection and monthly closing. |
| **Pre-condition** | 1. Date of Month End should be set up in Calendar Maintenance before the Month-End process starts. 2. Sales Closing (11th day of the previous month to the 10th day of the current month) and Statement generation was already processed. 3. Hold the batch jobs inside the Daily Batch Subsystem and release after the End of Month Run. |
| **Process** | **HOST Operator**   1. Confirms Date of the Month End Process 2. Prepares the List of the Jobs that will be processed 3. Starts Batch   **HOST**   1. Runs Monthly Job Steps 2. Selects customers for statement generation 3. Generates Customer Information 4. Performs Payment Closing 5. Generates Collection Reports 6. Performs Monthly Closing 7. Generates Collection Interface File   **HOST Operator**   1. Monitors Month Run while ongoing |
| **Stand-In Process** | Not applicable. |
| **Result** | 1. Backup Files will be created. 2. The following Reports will be generated:    1. List of Credit Balance (Branch Total)    2. List of Credit Balance (Brand Total)    3. Monthly Collection Report (Branch Break)    4. List of Credit Balance (Affiliated Break)    5. Statement File    6. Handling Charge List of Credit Balance (Branch Total)    7. Monthly Uncollection Report (Branch Break)    8. Handling Charge List of Credit Balance (Affiliated Total)    9. Handling Charge List of Credit Balance (Brand Total) 3. The following Database will be updated:    1. Balance History    2. Payment    3. Customer Information    4. Monthly Closing    5. Job Control    6. Collection Interface    7. Expiry Renewal |
| **Remarks** | **List of Monthly Jobs**   1. Backup Before Closing 2. Payment Closing 3. Backup After Payment Closing 4. Monthly Closing 5. Director Closing  * Director Closing * Credit Loss Closing  1. Card Collection  * Collection Interface File Output * Collection Payment History Pattern  1. Set Up Pre-Closing Data 2. Card Finance Reports 3. Expiry Card Renewal  * Expiry Card Renewal Data Select * Expiry renewal create embossed  1. Interest Group & Code Change 2. Monthly Closing Statement  * List of Credit Balance Error List * Card System Monthly Closing After Backup * Monthly Closing Statement  1. Card Backup After Monthly Closing |

## FR011 Payment



|  |  |
| --- | --- |
| **Overview** | The process defines how payment made by the customer at AEON branch, bank or convenience stores will be capture and store in the AFIS system. Online posting or allocation of payment will be implemented in AFIS. Payment Priority distribution will be as follow: Personal Loan, Hire Purchase, Credit Instalment, Cash Advance and Credit Purchase. |
| **Pre-condition** | 1. Customer received Statement. 2. Customer made payment in any of the following:    1. Branch Counter    2. Convenience Store    3. *Accredited Partner Banks*    4. *Payment Center* 3. Payment Allocation Priority has been defined. |
| **Process** | **Customer**   1. Make a payment based on the statement he receives.   **ACS-Cashier**   1. Accepts payment from Customer or from external partners. 2. For payment made thru external partners, Cashier performs a payment reconciliations and upload the received payment into the system. 3. For payment received directly from the Customer, cashier encodes the payment information into the system   **AFIS**   1. Stores or saves the payment information 2. System determines the purpose of payment.    1. If payment is intended only for payment of credit card transactions, system generates a payment interface file and sends to Credit Card system at the end of day.    2. If payment is for payment of Personal Loans, Hire Purchase and Credit Card transaction, system will first appropriate the payment to Personal Loans and Hire Purchase transactions. The remaining payment will then be allocated to Credit Cards transaction. System will create a payment interface file for the remaining payment and sends to Credit Card system at the end of the day. |
| **Stand-In Process** | Not applicable. |
| **Result** | * For Credit Card Transaction, a corresponding payment interface file will be created. * For Personal and Purpose Loan, online payment appropriation will happen |
| **Remarks** | * Payment Allocation Priority should be defined * A customer that pays minimum amount and “short payment” will not be subject for collection. |

# NON-FUNCTIONAL REQUIREMENTS

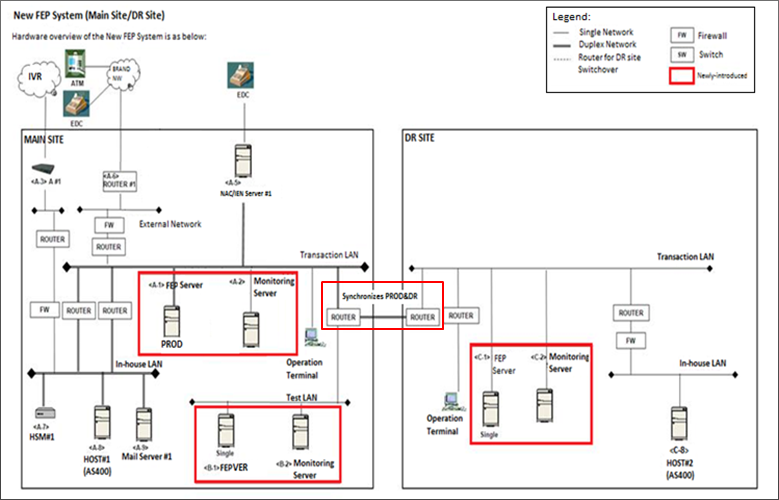


## Certification / Central Bank Audit Requirements

* ACSKH Credit Card System is required to pass the necessary Card Brand Certification for the following:
  + 1. Online Transactions
    2. Settlement and Clearing
* ACSKH Credit Card System is required to pass necessary audit requirements required by Cambodia’s governing body on Credit Card Companies.
* Third-party auditor in case the Cambodia does not have the Central Bank Audit requirement.

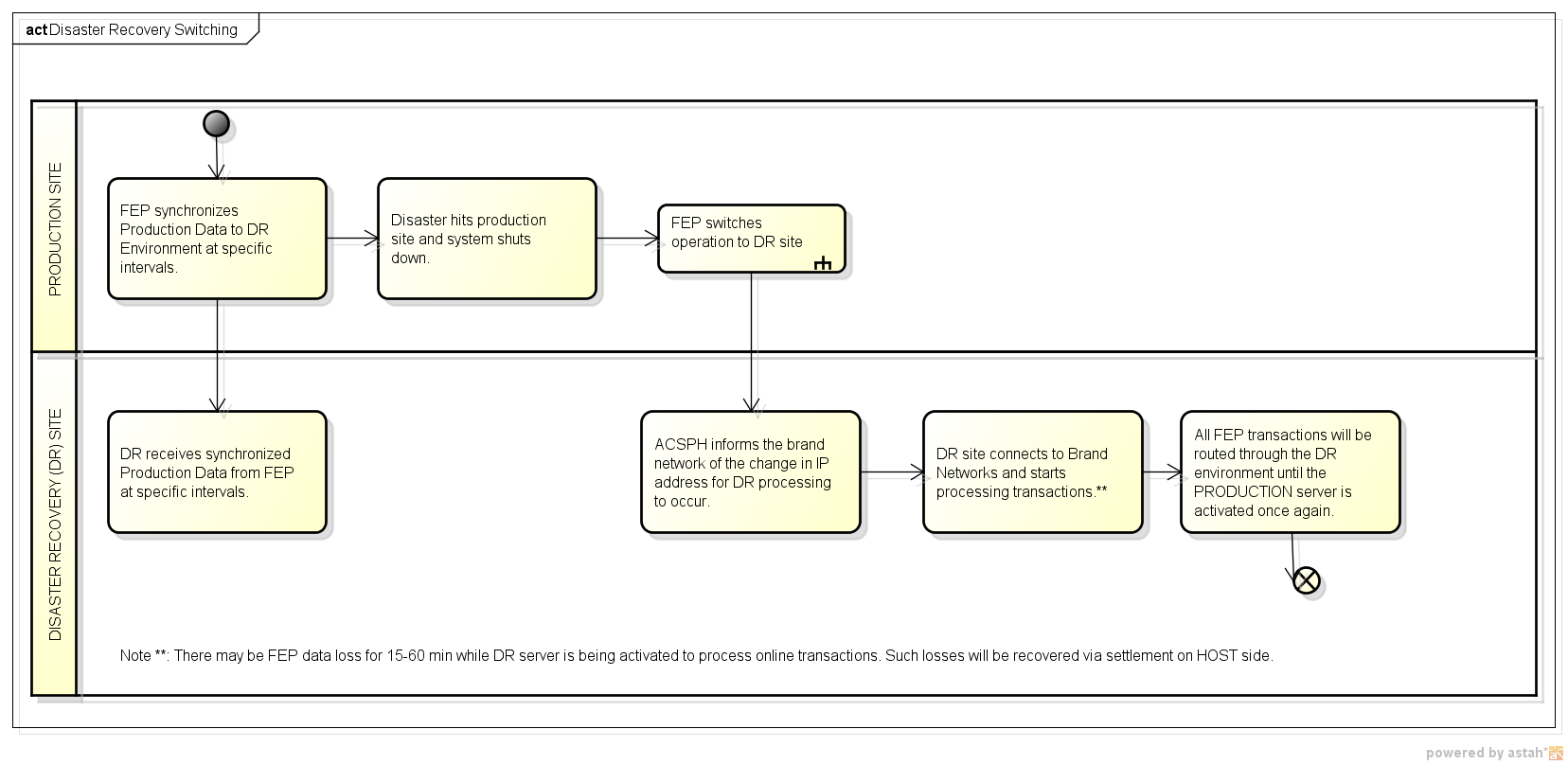
## Reliability

* Detect error earlier and keep the system operational (and the operation stable).
* Have disaster recovery site to continue business operation in case of site disaster.



**Note:**

For HOST Servers, Mimix 3rd-party data replication software needs to be installed (total 2 licenses) at both Prod and DR machines in order to perform automated data synchronization.



***Note:*** Switching from Main Site to Disaster Recovery site is ACSKH management’s decision based on implemented Business Continuity Plan.

## Performance

ACSKH Credit Card System shall be able to handle volume of transactions without affecting the performance of the system. The amount of transactions in Transaction-Per-Second (TPS) that New FEP and HOST system should handle shall depend on the hardware specifications of the system.

***Note:*** ACSKH’s current hardware specification is based on Indonesia’s setup plus a list of upgrades.

## Security

ACSKH Credit Card System shall be compliant with PCI-DSS requirements with regards to all security aspects.

## System Operations and Maintenance

* The system shall run for 24 hours and 365 days continuously.
* Current system for HOST and AFIS does not support Auto-Switching (Clustered Implementation).
* New FEP supports Auto-Switching (Clustered Implementation).

# Assumptions and Dependencies

The ACSKH Credit Card System that will be implemented in Cambodia will be composed of the following subcomponents:

* 1. New FEP System
  2. HOST System
  3. AFIS

All of which will be provided by ACSS.

**Note:** Core System will be based on ACS Malaysia system logic, Indonesia Infrastructure, the new ACSS Common Credit Card Infrastructure, plus certain programs/functions specifically enhanced or modified to meet ACSKH user requirements.

Finalization of the Credit Card System will depend on ACSKH Management’s final decision on how to implement this. Modules/Functions that will be dependent on the following sub-systems will have to be modified should there be any change required that would deviate from the current AS400/Host implementation.

# Information and Approval Section

Document Preparation:

|  |  |  |
| --- | --- | --- |
| **Person – In – Charge** | **Team** | **Signature / Date** |
| Karen Labustro | FEP |  |
| Faylenne Jaurigue | HOST |  |
| Ernesto Lanorio Jr. | AFIS |  |

Reviewed and Noted by:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| **Jhoycee Cruz** |
| ACSKH Project Director |

Reviewed and Verified by:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
|  |
| **Kathleen Umali**  Quality Assurance Section |

Approved by:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| **Jerome Alabat** |
| CCSDD Department Manager |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| **Filemon Elloso** |
| SDD Department Manager |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| **Alejandro Sison** |
| FEP Department Manager |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| **Takuya Ikitsu** |
| FEP Account Manager |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| **Takashi Komada** |
| HOST Account Manager |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| **Chikafusa Nagai** |
| ACSS President |