

NATIONAL PAYMENTS CORPORATION OF INDIA

**Interface specification for
Interoperable UID Based
Financial Inclusion
Architecture**

Ver. 2.0

May 28, 2010

Table of Contents

CHAPTER 1	INTRODUCTION	3
1.1	EXECUTIVE SUMMARY	3
1.2	SCOPE OF THIS DOCUMENT	3
1.3	AUDIENCE	3
CHAPTER 2	UID IMPLEMENTATION FOR FI ARCHITECTURE	4
2.1	ARCHITECTURE DIAGRAM AND BRIEF	4
2.2	INTERFACE SPECIFICATION	9
2.2.1	<i>System Definitions</i>	9
2.2.2	<i>Data element processing rules</i>	10
2.2.3	<i>Message format</i>	10
2.2.4	<i>Data Element Definitions</i>	13
CHAPTER 3	CHANGES FOR MEMBER BANKS AS ACQUIRER AND ISSUERS	23
CHAPTER 4	SETTLEMENT AND RECON	24
4.1	SETTLEMENT AND RECON	24
4.2	DISPUTE MANAGEMENT CYCLE	24
CHAPTER 5	RISK MANAGEMENT	26
CHAPTER 6	EXCEPTION CONDITIONS	27

May 28, 2010

Chapter 1 Introduction

1.1 Executive Summary

National Payments Corporation of India (NPCI) is formed to switch all the retail payments and fund transfer transactions in India from a central Infrastructure. Vision and formation of NPCI is backed by regulators and Indian Banks Association (IBA). NPCI has defined business lines to process in country interbank transactions for ATM, POS, 24*7 Remittance, ACH and CTS.

Government of India has initiated unique identification project for citizens of India. It is envisaged to use the UID schema and infrastructure for the financial inclusion in India. To enable the customers to use UID for the financial transaction across the payment networks in the country, NPCI proposes to facilitate routing of transactions to the central repository of UIDAI for user authentication through a single interface.

This interface document is targeted to achieve inter operability between banks for UID enabled financial inclusion transactions

NPCI shall allow banks to connect using this interface. FI organizations can connect on behalf of member banks to NPCI central infrastructure.

Interface with UIDAI Systems is out of the scope of this document, it will be directed by UIDAI in due course.

1.2 Scope of this document

This document serves as an UID addendum to NPCI's Host-to-Host Interface Specification. This document covers detailed description of the data elements in the ISO 8583 standard payment message specifications.

1.3 Audience

This document is a property of NPCI and should be not be circulated to external party without prior approvals of NPCI management team.

This document will be circulated to NPCI management team, NPCI Technical Advisor Committee, Business user group (to be formed) from member banks, different working groups established as directed by RBI and IBA.

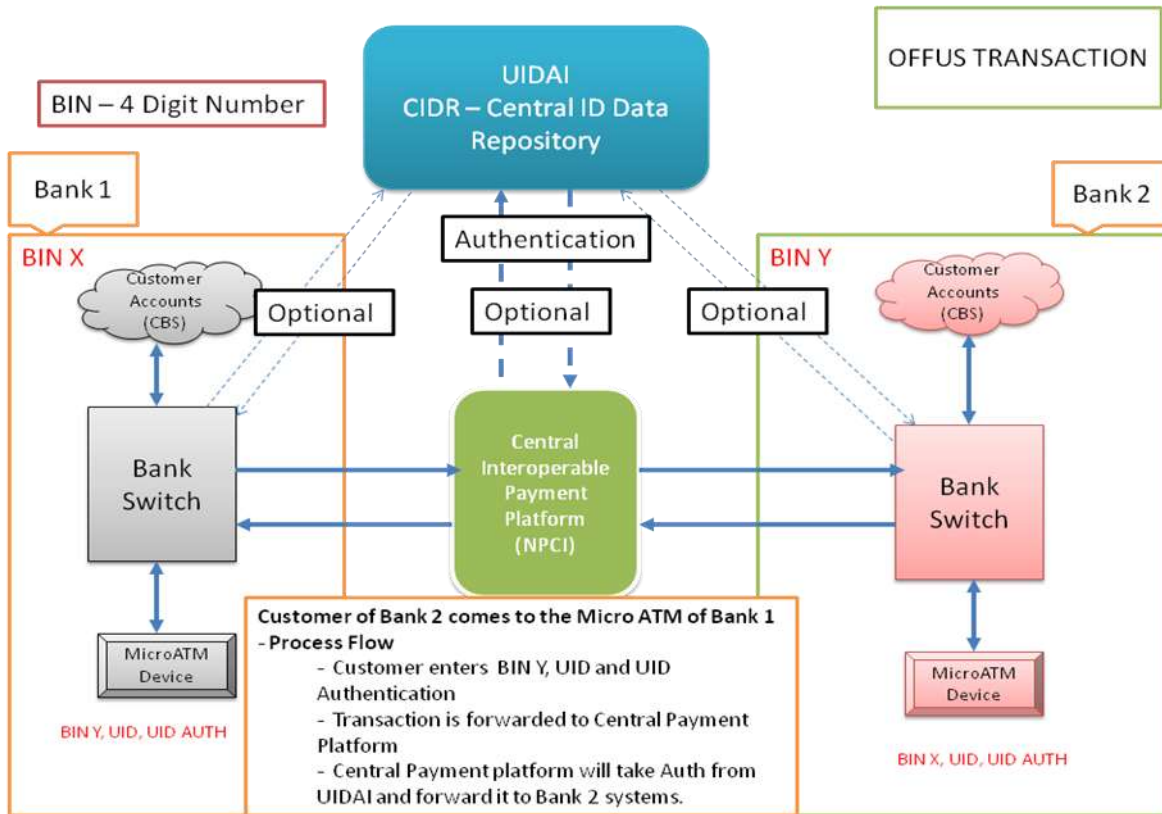
Chapter 2 UID Implementation for FI Architecture

2.1 Architecture Diagram and Brief

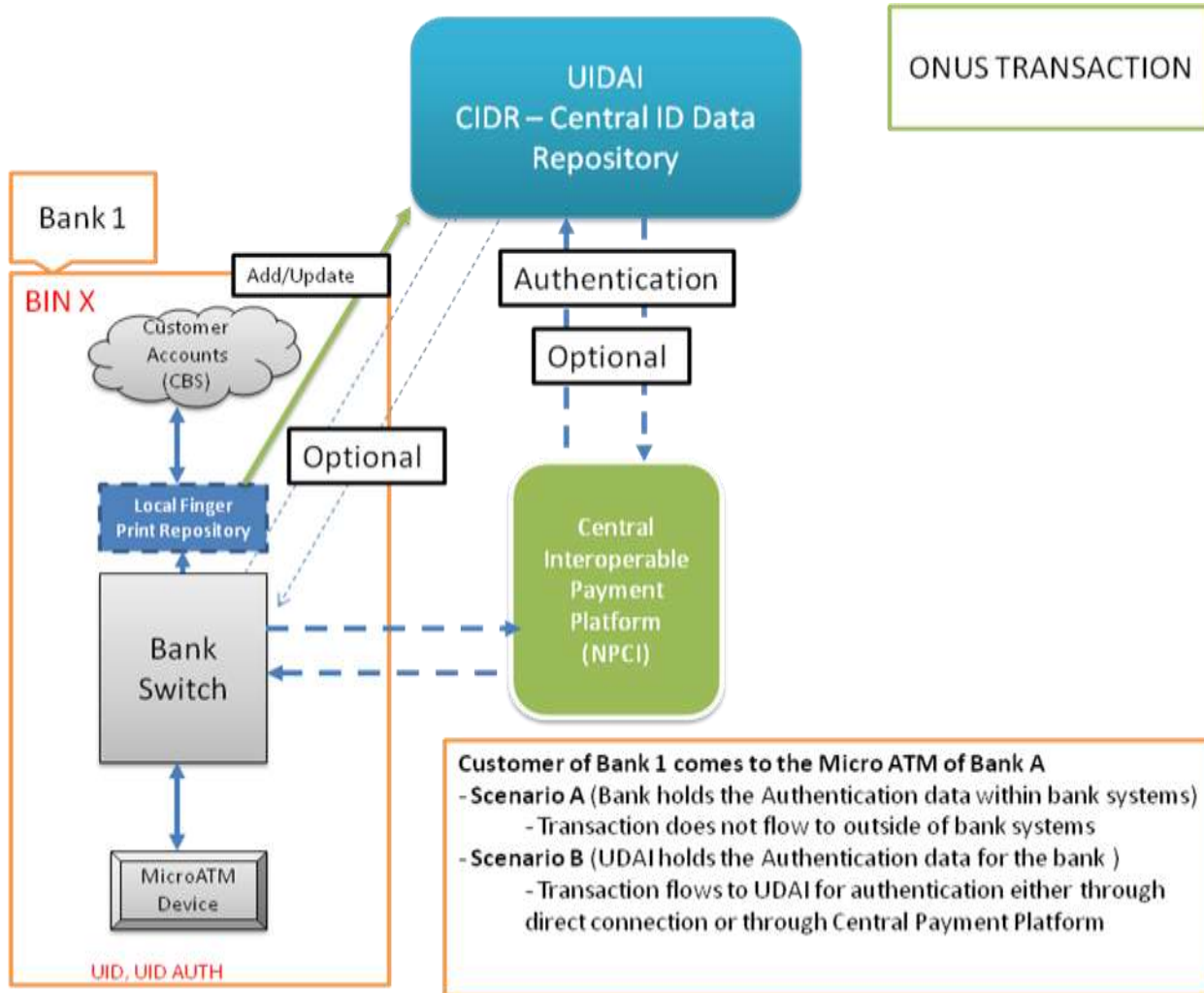
NPCI switch will be enhanced to support interbank transactions. For Onus Transactions only the authentication support will be provided based on the request from the issuer bank.

Following is the transaction Set,

1. Cash Withdrawal
2. Balance enquiry
3. Deposit
4. Funds Transfer
5. Authentication (only for on-us transaction)



May 28, 2010

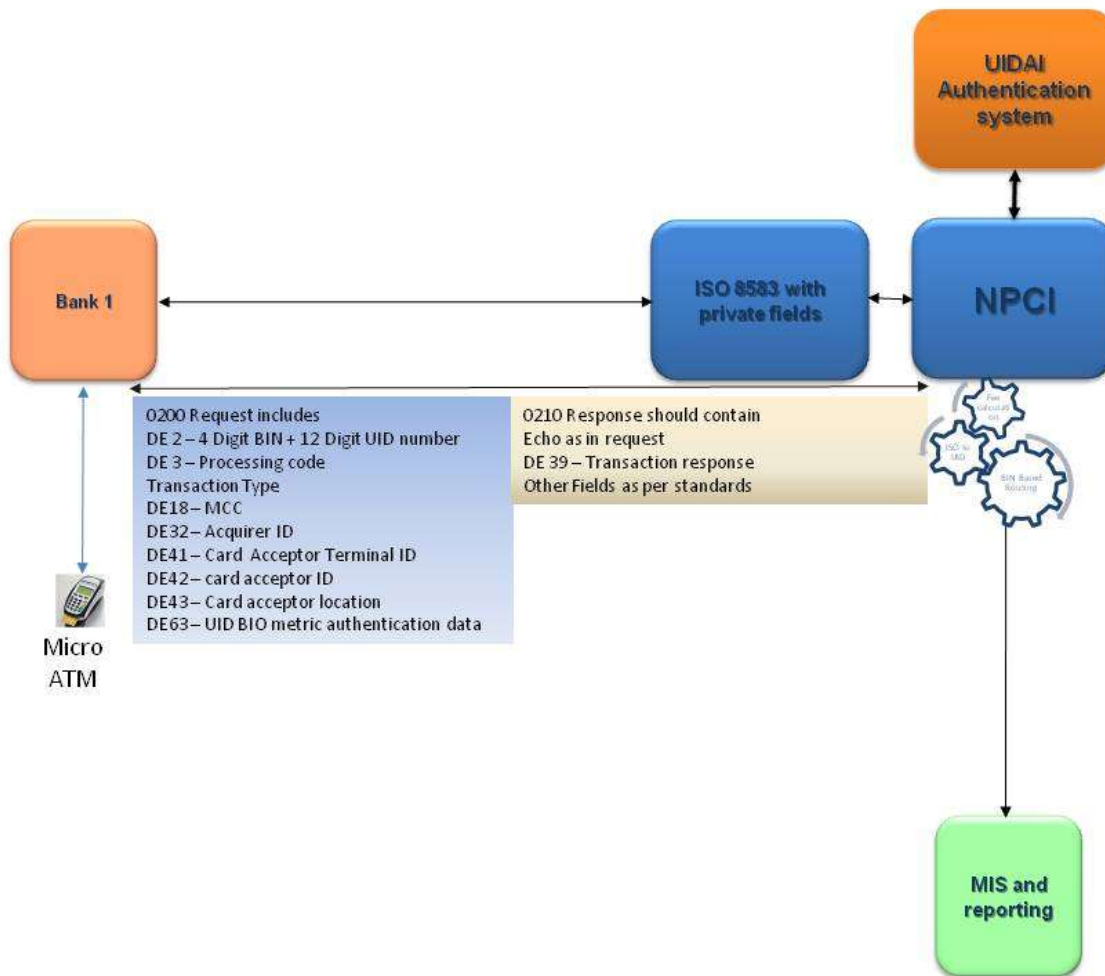


NPCI will have an interface with the central repository of UIDAI for the finger print authentication. This interface can be leveraged by the member banks that do not store finger print information or do not have interface with UIDAI central repository.

It is not mandatory that transactions will flow to UIDAI systems for authentication, and this situation only arises if banks are unable to store the data on their systems

Details – Onus Flow (only authentication)

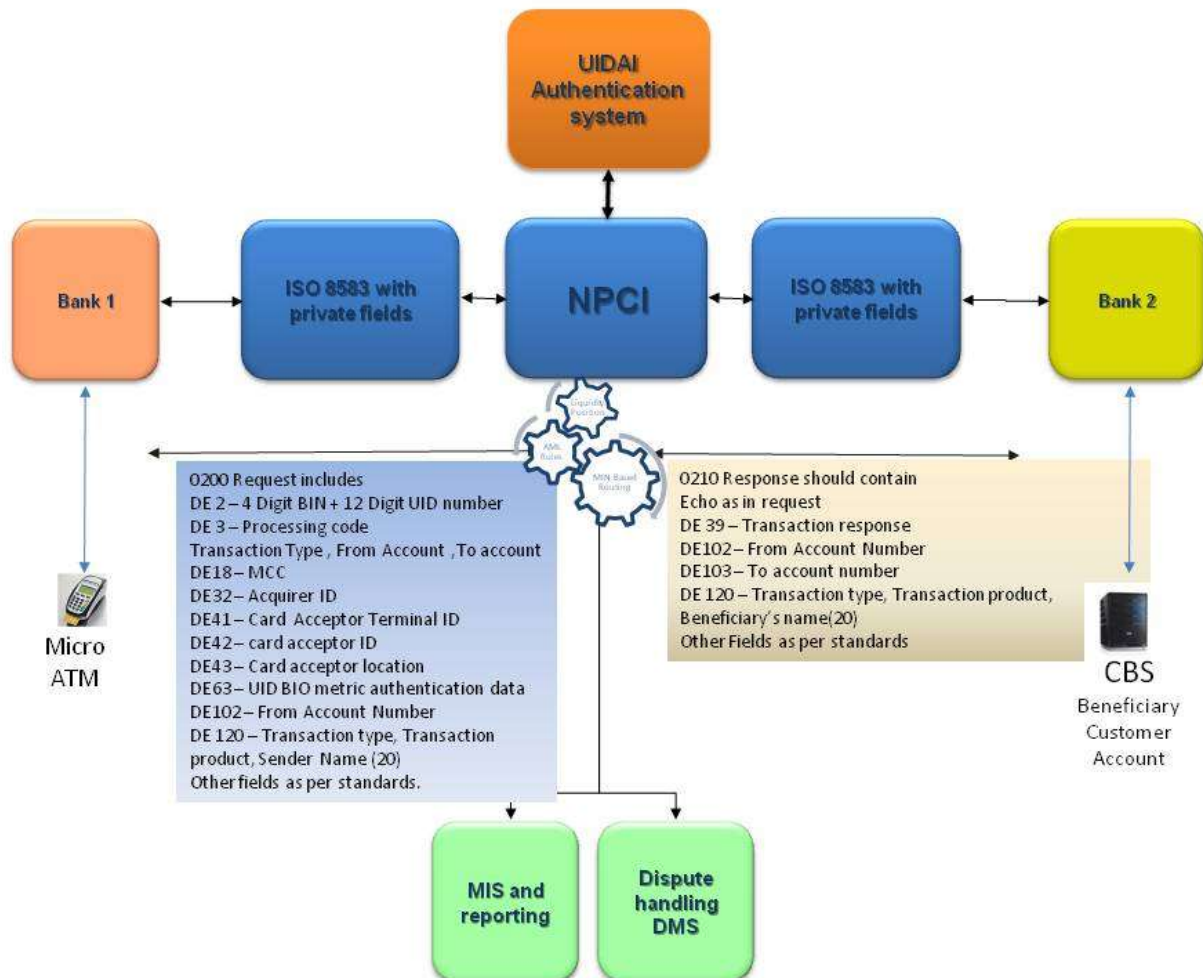
May 28, 2010



In case Bank does not hold the biometric information of customers and desires to leverage NPCI interface for UID authentication, above the transaction flow given where the transaction for biometric verification will be sent for requisite fields and verification result from UID will be forwarded to the bank. Otherwise this transaction is not visible to NPCI or UIDAI.

May 28, 2010

Details - Off us flow for Funds Transfer:



The transaction flow is depicted above for funds transfer from account of customer of Bank 1 to Bank2 where the transaction is initiated on Bank 1 terminal.

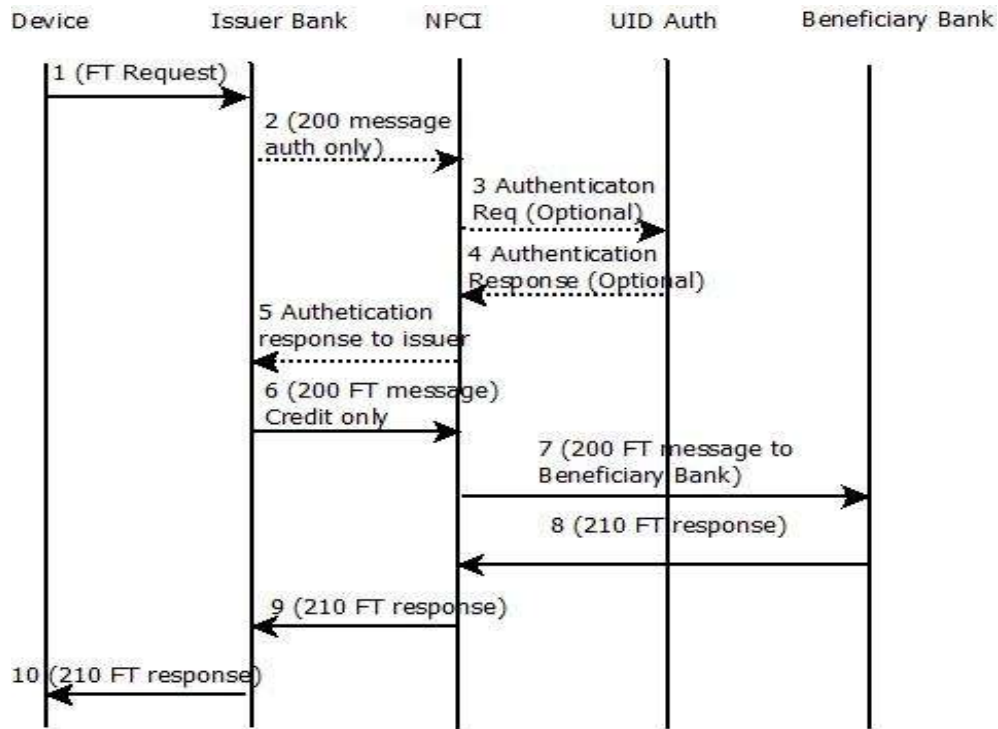
Online Debit and Online credit is envisaged in this transaction and beneficiary bank is expected to respond with beneficiary's account number and name in the response message.

Interchange will be provided by NPCI along with Bio Metric verification from UID system (required only in the case issuer bank does not store the bio metric data of customers in their systems or opt for authentication through NPCI)

UID to UID based fund transfer will be part of this Lab PoC. It is assumed for fund transfer that only pre authorized transaction (credit leg) will come to NPCI.

Possible scenarios for fund transfer are depicted below:

May 28, 2010



It is assumed that for fund transfer transaction sender will use its own bank micro ATM / POS / Infrastructure (Acquirer and Issuer are same)

All fund transfer transactions will pre- authorized by the issuer i.e. after debiting the sender account credit transaction will be sent to NPCI for processing. If any member bank is taking authentication service from NPCI, then the fund transfer transactions will be two step process as explained below:

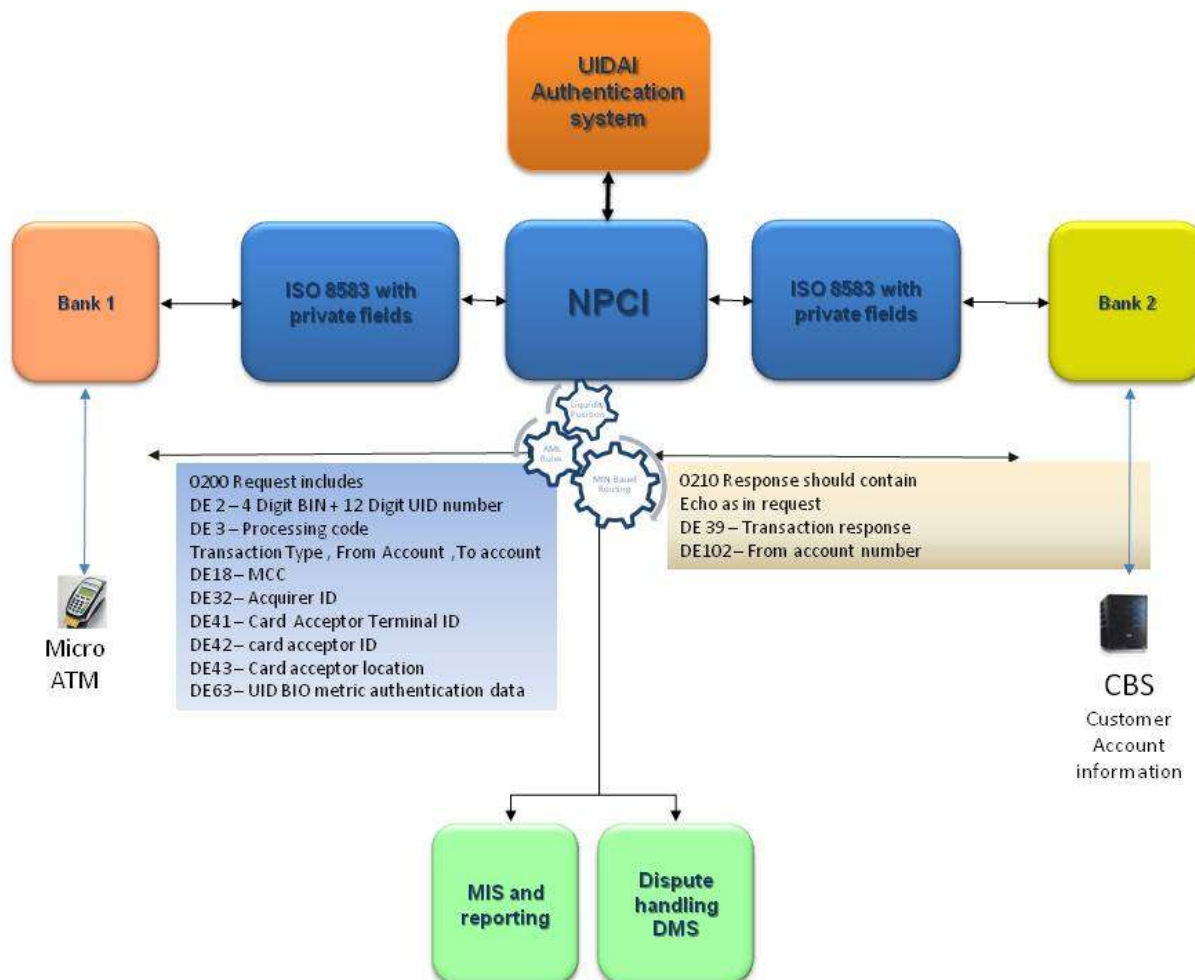
1. As shown in the above diagram (dotted line) authentication transaction will be initiated by the acquirer for authentication and subsequent debit to the sender account. Please note that authentication transaction is a non-financial transaction.
2. Once the debit to sender account is successful a remittance transaction is sent to NPCI. The context of both the transaction will be maintained by the acquirer.
3. The context of both authentication and fund transfer transaction will be maintained by the acquirer.

Note:

1. In case of authentication request, DE2 should be the remitter's UID number (Sender UID).
2. For fund transfer request data element DE2 will contain the beneficiary UID, DE120 will contain the sender UID and DE63 contains the biometric data of sender. It is the responsibility of issuer to debit the sender's account and send a fund transfer message to NPCI. The description of DE120 is detailed in Data Element Definition section.

May 28, 2010

Details - Off us flow – Other transactions (Cash Withdrawal, Deposit, balance Inquiry)



The transaction flow depicted above is for balance inquiry, Cash withdrawal and deposit transactions acquired on bank 1 terminal for bank2 customers. Interchange will be provided by NPCI along with Bio Metric verification from UID system (if required only in the case issuer bank does not store the bio metric data of customers in their systems)

2.2 Interface Specification

This document provides clear understanding of online interfaces, protocols and messages used, to enable implementation of the interface connection, and to serve as a basic document for future enhancements. Unless indicated otherwise, this document addresses ISO-8583:1987 standard for financial transaction messages.

2.2.1 System Definitions

May 28, 2010

Following points should be noted while developing the interface,

- I. Bank Systems and NFS systems will be connecting to each other using persistent socket connections.
- II. Bank will act as client and NFS will act as server.
- III. Banks will be responsible to generate the logon (0800 message type) message after every successful TCP socket connection.
- IV. NFS will generate cut over message (0800 message type) at 23:00 indicating business date change over.
- V. Banks and NFS will also generate Echo message (0800 message type) for keep alive during no transaction time. Ideal duration for the same should be 10 minutes.

2.2.2 Data element processing rules

Originator

The originator of the request message must be able to:

Correctly populate DE-2 comprising of 4 digit BIN and 12 digit UID number

Correctly populate DE-18 and DE-22 based on the data supplied by Acquiring touch point.

Correctly populate DE-63 with UID Bio metric data.

Populate DE-120 with Sender’s name for Fund transfer transactions.

NPCI

NPCI must be able to receive and process message containing DE-2, DE-63 and DE120.

Recipient

The Recipient must be able to receive and process messages containing DE-2, DE-22 and DE120.

It is up to the recipient how to interpret and use the values transferred in DE-22 & DE-120.

In fund transfer transactions, Recipient must populate DE-103 with “To account number” and DE-120 with Beneficiary’s name in the response message.

2.2.3 Message format

Message formats specified below contain UID related information. The changes in the message structure and/or data element content are indicated by bold characters. These formats supersede the Host-to-Host message specification provided by NPCI.

All message format definition tables use the symbols defined in the following table:

Message Types and Corresponding Data Elements	
Symbol	Meaning

May 28, 2010

Message Types and Corresponding Data Elements	
Symbol	Meaning
M	Mandatory.
M+	Mandatory, echoed from request.
C	Conditional.
C+	Conditional, echoed from request.
C*	Conditional, value may change.
O	Optional.
O+	Optional, echoed from request.
R	Reserved for future use.
-	Not used.

2.2.2.1 Administrative messages

Network Management Messages			
MTID	Data Element	0800	0810
1	Secondary bitmap	M	M
7	Transmission date/time	M	M
11	STAN	M	M
15	Date, settlement	C	C+
32	Acquirer institution ID	O	O+
39	Response code	-	M
48	Key Data (Optional – Dynamic Key Exchange)	M	-
64	MAC Code (Optional – MACing)	R	R
70	NMIC	M	M
128	MAC Code 2 (Optional – MACing)	R	R

2.2.2.2 Financial messages

Financial Messages			
MTID	Data Element	0200	0210
1	Secondary bitmap	C-	C
2	Primary Account Number	M	M+
3	Processing code	M	M+
4	Amount, transaction	M	M+
5	Amount, settlement	C	C+
7	Date/time, transmission	M	M
8	Fee, cardholder billing	R	R

May 28, 2010

Financial Messages			
MTID	Data Element	0200	0210
9	Conversion rate, settlement	C	C+
11	STAN	M	M+
12	Time, local transaction	M	M+
13	Date, local transaction	M	M+
14	Date, expiration	C	-
15	Date, settlement	C	C+
18	Merchant type	M	M+
22	POS entry mode	M	M+
25	POS condition code	M	M+
26	POS PIN capture code	C	-
32	Acquirer institution ID	M	M+
35	Track 2 data	C	-
37	Retrieval reference number	M	M+
38	Authorization number	-	C
39	Response code	-	M
41	Card acceptor terminal ID	M	M+
42	Card acceptor ID	M	M+
43	Card acceptor name/location	M	M+
49	Currency code, transaction	M	M+
50	Currency code, settlement	C	C+
52	PIN Block	C	-
54	Additional amounts	-	C
63	UID Authentication data	C	
64	MAC code	R	R
90	Original data element	-	-
102	Account 1 identification	C	C
103	Account 2 identification	C	C
120	Additional Data	C	C
121-123	Private use	C	C*
128	MAC Code 2	R	R

Reversal Messages			
MTID	Data Element	0420	0430
1	Secondary bitmap	C-	C
2	Primary Account Number	M	M+
3	Processing code	M	M+
4	Amount, transaction	M	M+
5	Amount, settlement	C	C+
7	Date/time, transmission	M	M
8	Fee, cardholder billing	R	R

May 28, 2010

Reversal Messages			
MTID	Data Element	0420	0430
9	Conversion rate, settlement	C	C+
11	STAN	M	M+
12	Time, local transaction	M	M+
13	Date, local transaction	M	M+
14	Date, expiration	C	-
15	Date, settlement	C	C+
22	POS entry mode	M	-
25	POS condition code	M	-
26	POS PIN capture code	C	-
32	Acquirer institution ID	M	M+
35	Track 2 data	O	-
37	Retrieval reference number	M	M+
38	Authorization number	C	C+
39	Response code	M	M
41	Card acceptor terminal ID	M	-
42	Card acceptor ID	M	-
43	Card acceptor name/location	M	-
49	Currency code, transaction	M	M+
50	Currency code, settlement	C	C+
54	Additional amounts	-	C
64	MAC code	R	R
90	Original data element	M	-
102	Account 1 identification	C	C
103	Account 2 identification	C	C
120	Additional Data	M	M+
121-123	Private use	C	C*
128	MAC Code 2	R	R

2.2.4 Data Element Definitions

DE-2 Primary Account Number, PAN

Format: LLVAR

Type: n..19

May 28, 2010

Description: The PAN number is the combination of 4 digit BIN number and the 12 digit UID number. It is mandatory for all 02xx and 04xx messages. Normal length of this field is 19 digits.

Field Edits: If present, it should be echoed in response and all subsequent messages. For all other transactions (including authentication transaction) except FT transaction, this field should have initiator's UID number. But for FT transaction, this field should have beneficiary's UID number.

Constraints: C: Element is present if DE-35 (Track 2) is not present.

Structure:

B	B	B	B	BR	BR	I	U	U	U	U	U	U	U	U	U	U	U	U
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

B – BIN (Bank Identification Number)

BR – Reserved for BIN (default value 0)

I – Indicator for UID – valid value 0 for UID.

U – Unique Identification Number of customer issued by UIDAI

Note – All Acquirers and Issuers will have to incorporate reserved digits for future use so that whenever NPCI sends addendums or circular without any changes in the systems it can be incorporated.

DE-3 Processing Code

Format: Fixed

Type: n6

Description: A series of digits that describes the type of transaction and the accounts affected by the transaction. It consists of three, two-digit subfields:

Digit 1 and 2: Transaction Code:

00	Purchase of goods/services
01	Cash withdrawal
10	PIN Verification (UID Biometric data verification/Authentication)
20	Credit, refund
21	Deposit
22	Credit adjustment
31	Balance inquiry
45	Fund Transfer
90	Extended transaction type**

Digit 3 and 4: From Account Type*

00	Unspecified/unknown
10	Savings
20	Checking
30	Credit card

May 28, 2010

Digit 5 and 6: To Account Number*

00	Unspecified/unknown
10	Savings
20	Checking
30	Credit card

Summary of processing code used for UID based transaction.

Cash withdrawal – 010000
Balance inquiry – 310000
Deposit – 210000
Finger print authentication – 100000
Fund Transfer – 900000¹

It is mandatory for all 02xx, 04xx messages.

Notes: * Other values may be used for optional features.

Field Edits: If present, it should be echoed in response and all subsequent messages.

Constraints: None

DE-18 Merchant Category Code (MCC)

Format: Fixed

Type: n4

Description: MCC is four-digit code in accordance with the Visa/MasterCard MCC definitions. The data element is mandatory for 02xx request messages. It is never present in response messages.

The proposed values are

6012 – Micro ATM UID transactions

(If member banks want to support UID transactions through their biometric ATMs then it will be 6011).

6010 – for regular POS device.

Field Edits:

Constraints:

DE-22 Point of Service Entry Mode

Format: Fixed

Type: n3

¹ See also DE-120 description for actual processing code

May 28, 2010

Description: The code describing the way PAN and PIN are entered at a touch point.

Data element consists of two sub-fields:

PAN Entry Mode

- 01 Manual**
- 02 Magnetic stripe read.
- 05 ICC.
- 90 Full and unaltered magnetic stripe read (enables CVV validation).

PIN Entry Mode

- 0 Unspecified.
- 1 PIN entry capability.
- 2 No PIN entry capability.
- 6 PIN pad inoperative.
- 9 Reserved for private use**

The data element is mandatory for 02xx, and 04xx request messages. It is never present in response messages.

Field Edits:

Constraints:

DE-25 Point of Service Condition Code

Format: Fixed

Type: n2

Description: Two-digit code indicating conditions at touch point:

- 00 Normal.
- 01 Customer not present.
- 02 Unattended terminal (CAT, ADM).
- 03 Merchant suspicious.
- 05 Customer present, card not present.**
- 07 Telephone request.
- 08 MO/TO request.

Field Edits:

Constraints:

DE-32 Acquiring Institution Identification Code

Format: LLVAR

May 28, 2010

Type: n..11

Description: Identifies the acquiring institution for the transaction, or its agent. The value will be defined by the host. The data element is mandatory for 02xx, and 04xx request messages. It is optional for 08xx messages.

Field Edits: If present, it should be echoed in response and all subsequent messages.

Constraints: O: Member can choose whether to use DE-32 in 08xx messages or not.

Note - NPCI shall assign appropriate codes to the participating banks to be used in this field.

DE-37 Retrieval Reference Number

Format:

Type: AN12

Description: The reference, assigned by the acquirer, to identify a transaction uniquely. It remains unchanged for all messages throughout the life of a transaction and is used for matching original message with reversal and/or store/forward messages. The standard format of RRN is as follows:

YDDDHSSSSSS

Y – Year (last digit of current year)

DDD – Julian date of transaction

HH – Hour of transaction

SSSSSS – STAN of transaction (Same as in DE -11)

The data element is mandatory for 02xx, and 04xx request messages. The RRN can be used for the entire dispute management of the transaction lifecycle.

In verification request value of DE-37 should be same as original remittance transaction RRN

Edit Field: It must be echo back in response message

Constraint: None

DE-39 Response Code

Format:

Type: an2

Description: This code indicates the disposition of a message as detailed tables below.

Each code is associated with specific action code that is to be taken:

A Approve transaction.

D Decline transaction.

May 28, 2010

Field Edits: In reversal and store/forward requests, value identifies the reason for reversal or store/forward message.

Constraints:

The following is the addendum covering different scenarios for UID specific situations and appropriate Response codes supported for declined UID transactions in addition to the existing response codes referred in the NPCI Host-to-Host specification document.

0210 Response Codes			
Code (generated by)	Description	Action	Description
U1 (UID Auth system)	UID Finger print match error	D	The finger print does not match with the UID number.
U2 (UIDAI / NPCI)	UID data format error	D	The format of the UID data is not correct.
U3 (Issuer / UIDAI)	UID is not registered	D	UID is not present in the UID data base.
U4 (Issuer / UIDAI)	UID match error, suspected fraud	D	Finger print does not match and fraud suspected.
U5 (UIDAI)	UID general error	D	UID declines for unknown reason
U6 (NPCI)	UID system not available	D	UID system is not available
U7 (NPCI)	UID system time out	D	UID system does not respond in time.
U8 (Issuer)	No account for UID	D	Issuer bank unable to locate account number for UID
U9 (Issuer)	Restricted UID	D	Restricted UID marked as restricted at Issuer
UA (NPCI / UIDAI)	Suspected fraud	D	Issuer suspects fraud with specific UID
UB (NPCI)	Limited exceed by member bank Only for FT transaction	D	Limited exceed by member bank (Remitter bank) Only for FT transaction

DE-41 Card Acceptor Terminal Identification

Format: Fixed

Type: an8

Description: A unique code identifying the terminal at the acceptor location. Special characters (including national character support characters) are not allowed since some networks and/or back-office systems may have problems accepting these characters. The data element is mandatory for 02xx, and 04xx request messages.

Character 1-3 Bank code / FI code

Character 4-8 Unique Terminal ID

May 28, 2010

The first 3 digits of the terminal ID should be institution name.

Field Edits: If present, it should be echoed in response and all subsequent messages.

DE-42 Card Acceptor Identification Code

Format: Fixed

Type: an15

Description: Identifies the acceptor in a transaction and if the acceptor is different from the acquiring institution. Special characters (including national character support characters) are not allowed since some networks or back-office systems may have problems accepting these characters. The data element is mandatory for 02xx and 04xx request messages.

Field Edits: If present, it should be echoed in response and all subsequent messages.

Character 1-15 Merchant Name / Bank Correspondent Name

DE-43 Card Acceptor Name/Location

Format: Fixed

Type: an40

Description: The name and location of the acceptor (Touch Point), which defines the point of service in both local and interchange environments. Special characters (including national character support characters) are not allowed since some networks or back-office systems may have problems accepting these characters. Data element consists of the sub-fields detailed in the table below. The data element is mandatory for 02xx, and 04xx request messages.

Field Edits: If present, it should be echoed in response and all subsequent messages.

Character 1-25 Merchant Address / Bank Correspondent Address

Character 26-38 City Name

Character 39-40 Country Code (IN)

DE-63 Private Use Field 63 – UID Biometric Authentication Data

Format: LLLVAR

Type: an999

Description: This Element is encrypted containing finger print minutiae collected at the Micro ATM. Data may contain multiple minutiae or other UID authentication payload. UID/NPCI will come up with the PKI based encryption standards in a due course for this data element.

May 28, 2010

Field Edits:

Constraints: C: Data element is present for UID based 02xx request messages.

DE-90 Original Data Element

Format: Fixed

Type: n42

Description: This data element contains parts of the original message being reversed or adjusted and is used to match reversal/adjustment to previous authorization or financial transaction message(s). This data element consists of sub-elements which are described below:

Usage:

Field edits:

Constraints:

Sub-elements description:

Position	Length	Field Name	Description
01-04	4	Original MTID	MTID of original request
05-10	6	Original STAN	DE11 of original request
11-14	4	Original Local Date	DE12 of original Request
15-20	6	Original Local Time	DE13 of original request
21-31	11	Original Acquiring Institution ID	DE32 of original request
32-42	11	Not used (to be filled with zero)	--

Note: The Sender UID is sent in DE120 for reversal transaction.

DE-102 Account Identification 1

Format: LLVAR

Type: ans28

Description: A series of digits used to identify a customer account. It denotes the "From" account number involved in the transaction (e.g. the Debit account in withdrawal or transfer transaction). The account number in the Account Identification 1 field must be right justified with leading zeros.

Usage:

In the UID based Fund transfer transactions, issuer bank must send "from account number" which is debited for the transfer amount. The account number should be asked as per banks policy.

Field Edits: If present, should be echoed in all subsequent messages.

May 28, 2010

Constraints: C: The data element is used in 02xx, and 04xx messages, whenever account information must be transferred.

DE-103 Account Identification 2

Format: LLVAR

Type: ans28

Description: A series of digits used to identify a customer account. It denotes the “to” account number involved in the transaction (e.g. the credit account in deposit or transfer transaction. The account number in the Account Identification 1 field must be right justified with leading zeros.

Usage:

In the UID based Fund transfer transactions, beneficiary bank must send the Beneficiary’s account number to which the amount was credited.

Field Edits: If present, should be echoed in all subsequent messages.

Constraints: C: The data element is used in 02xx, and 04xx messages, whenever account information must be transferred.

DE-120 Additional Data

Format: LLLVAR

Type: an999

Description: These fields are Tag-based.

Usage:

The generic description of DE120 is as follows:

<Tag number><Tag length><Tag data><Tag number><Tag length><Tag data>...

Tag number size is 3, Tag length is represented as LLL and Tag data is as per requirement

UID to UID fund transfer request:

DE2 will contain sender UID

0200 message from acquirer / Issuer to NPCI (for FT acquirer and issuer are same)			
Tag	Description	Length	Value
001	Transaction type	2	45
002	Product indicator	3	UID
045 (optional)	Sender Name	20	Sender Name
060	Sender UID	20	Sender UID with BIN. Format

May 28, 2010

			BBBB000UUUUUUUUUUUUUU (refer DE2 structure)
0200 message from NPCI to beneficiary bank			
001	Transaction type	2	45
002	Product indicator	3	UID
045 (optional)	Sender Name	20	Sender Name
060	Sender UID	20	Sender UID with BIN. Format BBBB000UUUUUUUUUUUUUU (refer DE2 structure)
0210 message from beneficiary to NPCI			
001	Transaction type	2	45
002	Product indicator	3	UID
045 (optional)	Sender Name	20	Sender Name
046 (optional)	Beneficiary Name	20	Beneficiary Name
060	Sender UID	20	Sender UID with BIN. Format BBBB000UUUUUUUUUUUUUU (refer DE2 structure)
0210 message from NPCI to acquirer / issuer			
001	Transaction Code	2	45
002	Product indicator	3	UID
045 (optional)	Sender Name	20	Sender Name
046 (optional)	Beneficiary Name	20	Beneficiary Name
060	Sender UID	20	Sender UID with BIN. Format BBBB000UUUUUUUUUUUUUU (refer DE2 structure)

The sender and beneficiary name will be carried as a part of message but only sender and beneficiary UID will be stored at NFS system for record purpose.

Field Edits: The contents of field may change in responses depending on result of transaction.

Constraints: C: Must be present in UID based Fund transfer transaction.

May 28, 2010

Chapter 3 Changes for Member Banks as Acquirer and Issuers

1. Changes for Acquirer Members,

- a. Establish connection with Micro ATM switch.
- b. Addition of new transaction in the interface to existing NFS Switch
- c. Changes in the current recon system to reconcile the interchange and switching fees for UID based transactions.

2. Changes for Issuer Members,

- a. Addition of new transaction in the interface to existing NFS Switch
- b. Changes in the current recon system to reconcile the interchange and switching fees for UID based transactions.

3. Changes in NPCI systems,

- a. Establish interface connection with CIDR – Central ID data repository only for the banks which does not store the authentication data. (This is Optional)
- b. Addition of new transaction in existing NFS switch
- c. Changes in online dispute management system for new rules
- d. Changes in billing system for these new transaction types.
- e. Changes to develop new reports and raw data files.

Chapter 4 Settlement and Recon

4.1 Settlement and Recon

Following are the changes in the settlement and recon process,

1. Addition of these transaction in the existing acquirer raw data file and issuer raw data file circulated by NFS operations team to member banks.
2. Addition of this transaction in the existing acquirer activity report and issuer activity report circulated by NFS operations team to member banks.

4.2 Dispute Management Cycle

Following are the changes in the settlement and recon process,

1. NPCI will also form an arbitration committee with nominated members of member banks to decide on member banks. **
2. Dispute Cycle
 - a. Debit/Credit Adjustment. (Acquirer Initiated)
 - b. 1st Chargeback (Issuer initiated)
 - i. Optional proof to be submitted – Scanned copy of the customer dispute letter.
 - c. Representment (Acquirer Initiated)
 - i. Document proof of visible scanned copy of the charge slip or Micro ATM journal.
 - d. Arbitration (Issuer Initiated)
 - i. Issuer can initiate the arbitration and on this decision will be taken by the team responsible.
3. This transaction cycle will following timelines,**
 - a. 1st chargeback - Issuer needs to raise this within 120 days from the transaction date.
 - b. Representment – Within 10 days of the receipt of the chargeback for acquirer needs to represent.
 - c. Credit Adjustment – Acquirer can raise this within 30 days from the transaction date.
 - d. Debit Adjustment – Acquirer can raise this within 10 days from the transaction date.

May 28, 2010

4. Separate additional report for only UID based transactions for acquirer and issuer banks.
5. Settlement cycle for all these transactions will be 23:00 to 23:00 for all days as per the current NFS settlement windows.
6. These transactions are treated as SMS (Single Message System) so will settle each day after successfully processed irrespective of the merchant settlement on the device.

**This approach will be discussed and finalized in Business User Group meeting.

Chapter 5 Risk Management

Following will be the risk management done by all the member banks,

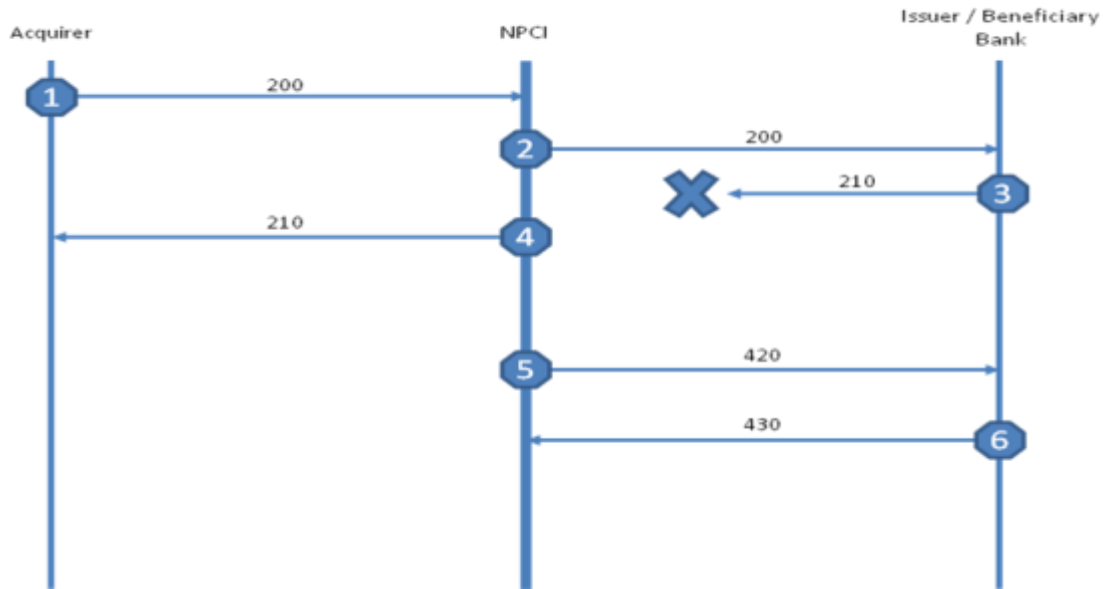
1. Issuer Bank will be responsible to do all the following checking,
 - a. Balance authorization
 - b. Account Validations/Verifications.
 - c. Number of Transactions in a day for the specific Account product
 - d. Maximum limit in a day for the specific card product
 - e. Issuer banks will either not store the UID authentication data or store it in encrypted formats as per PCI guidelines.
 - f. AML related validations for Funds Transfer transaction.
 - g. Fraud Check
 - h. Duplicate (Multiple) reversals and original transactions.
 - i. All other validations
 - j. Issuer bank will connect to NPCI network on IPSEC/VPN.

2. Acquirer Bank will be responsible for following checking,
 - a. Acquirer shall not log the Biometric data on the switch.
 - b. Transaction and incoming message validation coming from Micro ATM.
 - c. Ensure card entry mode and pin entry mode to be present in the request.
 - d. Unique key management for the terminals.
 - e. Acquirer banks will either not store the UID authentication data or store it in encrypted formats as per PCI guidelines.
 - f. Issuer bank will connect to NPCI network on IPSEC/VPN

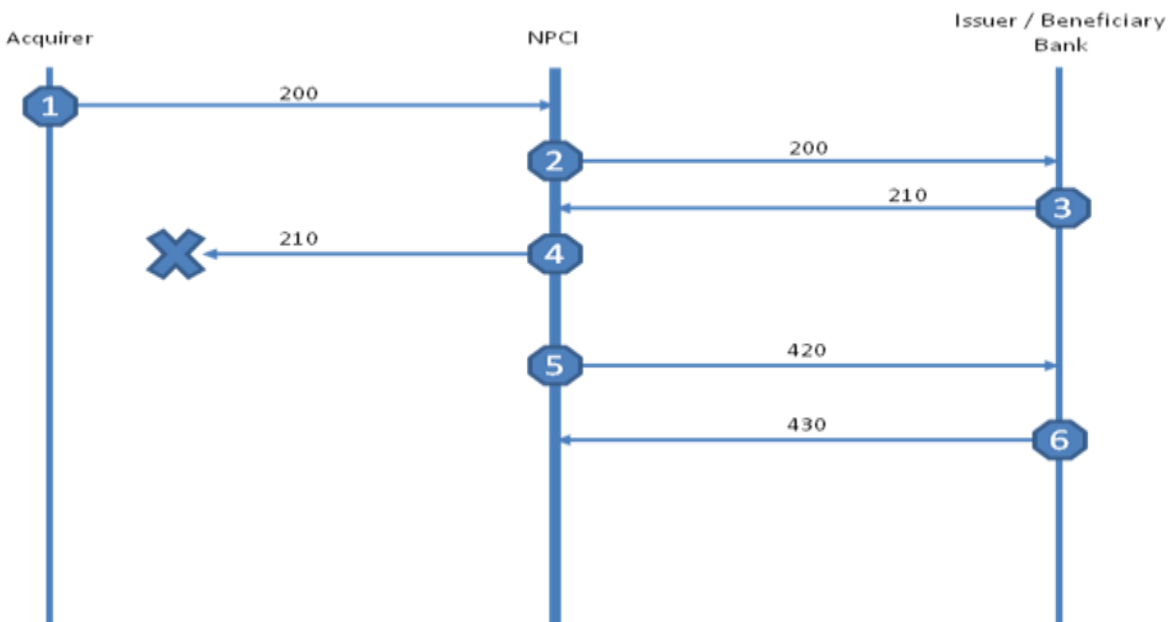
Chapter 6 Exception Conditions

Exception conditions for which reversals would be generated.

Cash Withdrawal Exception



Cash Withdrawal Exception



Please make the change on above flow. In case of time out acquire should initiate a rerversal.

May 28, 2010

Cash Withdrawal Exception (Time out)

