BANKSERVAFRICA

SADC TCIB INTERFACE SPECIFICATIONS

19 SEPTEMBER 2019 **VERSION 2.3**

PO BOX 62443, MARSHALLTOWN, 2107
TEL: +27 11 497 4000 / FAX: +27 11 493 0595

BANKSERVAFRICA

CONTENTS

BANKSERVAFRICA

SADC TCIB Interface Specifications

The SADC Transaction Cleared on an Immediate Basis is a cross border real time credit transfer system that relies on network connectivity, authentication mechanisms, process flows and API interface specifications detailed in this document.

1. VERSION CONTROL

Version No.	Date	Description	Author
1.0	January 2019	Version 1.0	Martin Suchecki
2.0	March 2019	Only included information relevant to Incubation Phase	Martin Suchecki
2.1	June 2019	Included STATUS API via POSTMAN	Martin Suchecki
2.2	June 2019	Message ID and transaction ID must be unique	Martin Suchecki
2.3	October 2019	Use MDM to determine SPID when processing through a hub. Included Integration diagrams	Martin Suchecki

2. GLOSSARY OF TERMS

AML/KYC	Anti-money Laundering / Know-your-Client
API	Application Program Interface
BIC	An international Bank Identification Code allocated by SWIFT
CAT	Central African Time
cURL	Client URL. Curl is a command-line tool for transferring data using various protocols.
HSRP	Hot Standby Routing Protocol
GMT	Greenwich Mean time, also know as Coordinated Universal Time UTC
IKEv2	IKEv2 (Internet Key Exchange) works by using an IPSec-based tunneling protocol to establish a secure connection
IPSEC	Internet Protocol Security, used to provide a secure tunnel across a public network
IP SLA	Internet Protocol Service Level Agreement, used to collect information about network performance in real time
Lean Build	Incubation phase for take on of clients
Mark Off File	Transaction list of processed transactions for participants
MDM	Master Data Management
MMSP	Mobile Money Service Provider
MNO	Mobile Network Operator
MSISDN	Mobile Station International Subscriber Directory Number
PPSP	Payment Processing Service Provider
S2S	Site to site
SPID	Scheme Participant Identification
TCIB	Transactions Cleared on an Immediate Basis
TLS	Transport Layer Security
TTL	Time to Live. This limits the lifespan of a message on a network.
URL	Uniform Resource Locator
VPN	Virtual Private Network
XML	Extensible Markup Language

3. INTRODUCTION

The low value Transactions Cleared on an Immediate Basis (TCIB) is a real time cross-border switch for immediate payments in the SADC region.

3.1. AUDIENCE

The specification is aimed at network, connectivity specialists and payment message originators at banks and non-banks authorised to submit and receive cross-border payment messages using the BankservAfrica TCIB real time switch.

This document contains network connectivity requirement for banks and non-bank participants to join the real time TCIB service.

Before reading this document, participants must ensure that they have engaged with the RCSO, their sponsoring banks and with the SADC RTGS and completed all agreements and met all requirements to participate in this service.

Banks must familiarising themselves with ISO 20022 pacs.004/008 XML schemas.

The document is technical and, to avoid repetition, makes reference to other documents where detailed information of processes are specified. This document must be read in conjunction with these other documents, which are listed below:

- TCIB Assent Agreement
- VPN Application Form
- TCIB Participant On Boarding
- TCIB Master Data Management
- TCIB Service Level Agreement and User Manual
- TCIB Change Request Procedure Manual
- TCIB Settlement Service manual
- Message Usage Guidelines
- Logging into MyStandards
- Using the Readiness Portal on MyStandards

3.2. SCOPE OF TCIB MESSAGING

The scope of requirements for real time payments includes:

- Real time messages used to make payments and payment returns
- Endpoint required for payments and payment return
- HTTP based messaging
- Process flows supporting real time payments
- Status API
- Timing requirements of payment legs
- Security requirements
- Processing cycles

3.3. EXCLUSIONS

This document only details specifications for the incubation phase.
Text that is in grey is not included in this phase.

3.4. ACTIONS REQUIRED OF PARTICIPANTS

Procedures for engaging with BankservAfrica are detailed in the **SADC RCSO - TCIB – On-Boarding** document.

A non-bank participant must have provided its settlement Bank details by currency to the SADC RCSO and completed all other actions as detailed in the SADC RCSO TCIB – On-Boarding document. Participants need to advise their settlement banks of such arrangements.

Details of participants are maintained on a Master Data Management system (MDM) at BankservAfrica, See **TCIB Master Data Management document**. During registration, BankservAfrica will issue a **Scheme Participant Identifier**, commonly known as a SPID.

If the participant wishes to transact through a processing hub, the participant's hub details will be captured with the participant details. This will indicate to other participants and to TCIB that payments and payment returns to that participant must be cleared and settled with the hub. The settlement will occur with the hub's settlement bank.

During the Incubation Phase, Master Data details will be held and distributed manually by BankservAfrica. MDM details during this phase will be distributed in comma delimited files.

The participant must use the ISO 20022 TCIB messaging standards for payments submitted to TCIB real time switch as detailed blow.

4. NETWORK CONNECTIVITY AND DATA FLOW

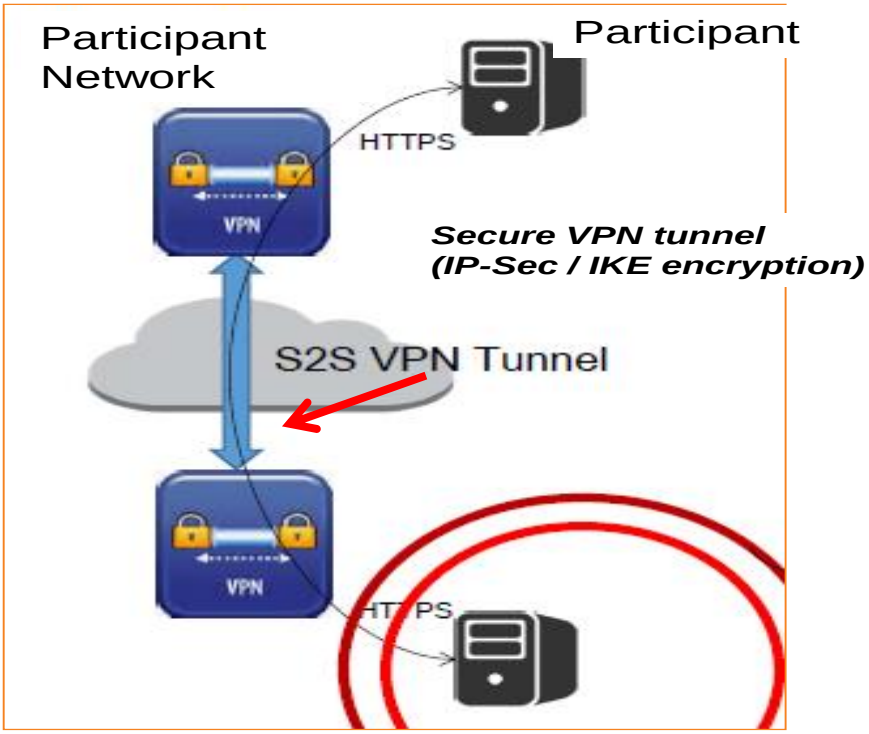
The participant must be registered with the SADC RCSO (see **SADC RCSO - TCIB – On-Boarding** document as part of this package) along with your PPSP (if applicable).

Connectivity must be established with BankservAfrica as detailed in documentation. A **TCIB – VPN S2S Application Form** must be completed. All fields are required for the Incubation Phase.

4.1. HOW TCIB PARTICIPANTS CONNECT TO THE BANKSERV TCIB SERVICE

A **VPN** tunnel (often simply referred to as a VPN, or virtual private network) is an encrypted connection between your computer and the wider Internet.

A secure Site-to-Site VPN tunnel bi-directional connectivity must be created between participants and TCIB real time switch, as depicted below:



The VPN communication link must be secured using IKEv2 encryption with IPSec-based tunnelling protocol.

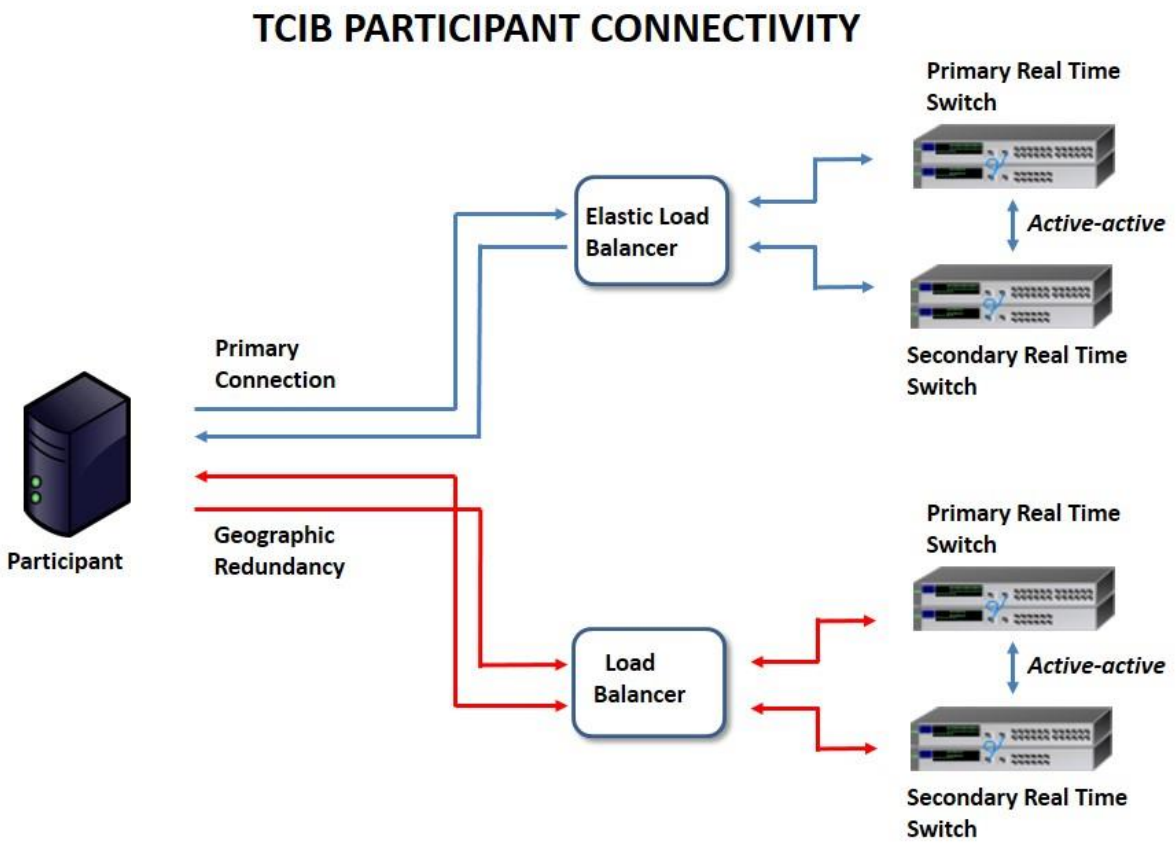
Registered participants will access the API using user name and password which will be issued and maintained by BankservAfrica.

4.2. CONNECTIONS TO PRIMARY AND SECONDARY SITES

Note that connections to Geographic Redundancy detailed in this section are not required for the Incubation phase. IP addresses of participants will be agreed for the Incubation Phase.

After Incubation Phase the ultimate connectivity requirements are detailed blow.

Participants are expected to have two connections to real time switch site, one as a sending participant and one as a receiving participant. In addition, participants may wish to have connections to both primary and geographic redundancy sites. If participants connect to both primary and geographic redundancy sites as senders and receivers, four connections are required as shown below.



Participants are expected identify themselves to the primary and/or secondary sites using echo messages (see paragraph on Echo message below). The real time switch must maintain a table of which participants are logged on an active.

Note that for the Incubation phase, only a primary connection is required.

4.3. ROUTING OF REAL TIME MESSAGES

The routing of the message is determined by BIC codes or SPIDs held in the payload of the HTTP message, see below. The payload contains a payment instruction in ISO 20022 format.

This message identifier <MsgId> is used by the message management component to control message delivery.

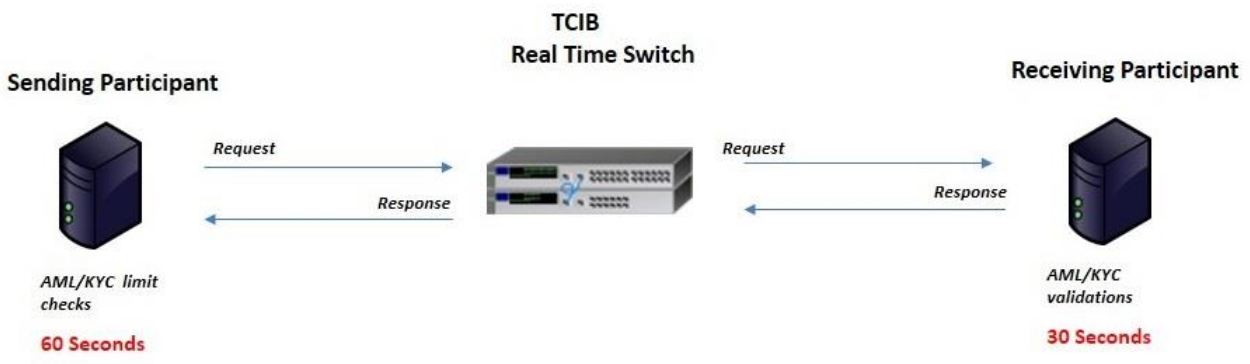
The End To End Identifier <EndToEndId> in the Credit Transfer is used to uniquely identify the payment from end to end. The End To End Identifier does not change as it passes through the switch. The End To End is used in a payment return message to identify the original payment.

When the transfer is to a bank account, TCIB Real Time switch routes the message to the participant identified by the Credit Agent Financial Institution Identifier <CdtAgtr><FinInstnId><BICFI> element. When the transfer is to a non-bank participant or mobile wallet, TCIB routes the message to the participant identified by Credit Agent Identification <CdtAgtr><FinInstnId><Othr><Id>. This element will contain the creditor Scheme Participant Identifier SPID. The Master Data Management (MDM) file contains the complete list of TCIB participants, their BIC codes (for banks) and SPID codes.

4.4. PARAMETERS REQUIRED FOR TCIB REAL TIME PROCESSING

Parameter	Value
Originating participant time out	5 seconds
TCIB Switch time out	5 Seconds
Destination participant time out	5 seconds
TCIB switch cut over time	24:00

4.5. TIMINGS FOR QUEUE MESSAGES AND APPLICATION PROCESSING



The sending participant must perform AML/KYC checks before sending a payment. This can take time and is not considered in message timings. The timing of the message starts when the request is sent.

The sending participant sends the payment request to TCIB Real Time Switch. The connection time on the network should be insignificant and if measured, the time will be in the order of milliseconds. If a connection is not made in 5 seconds, the sending participant times out.

The TCIB Real Time Switch makes a connection and sends the request to the recipient. The recipient makes a connection and sends a successful or unsuccessful response to the TCIB Real Time Switch. The TCIB Real Time Switch makes a connection and sends the response to the sending participant.

Timeouts are detailed in Section 6 below.

4.6. NETWORK SECURITY

All API interfaces between TCIB and participants are over HTTPS. BankservAfrica will provide a SSL certificate for all inbound APIs. The participant are expected to provide an SSL certificate for all outbound APIs.
Participants access TCIB APIs using user names and passwords which will be issued and maintained by BankservAfrica.
Participants are to provide APIs with user names and passwords for outgoing messages.

All Participants integrate into BankservAfrica's EIG (External Interface Gateway) systems which are hosted in the DMZ (De Militarized Zone) of TCIB's network.

For integration testing all access to inbound and outbound APIs are provided on staging systems. Once all API validations are through then inbound and outbound APIs are migrated to live production servers.

4.7. OPERATING TIMES FOR TCIB REAL TIME PROCESSING

For the Incubation phase, the transaction clearing/processing will take place as detailed in the table below

Start Time	End Time
08H00	14H30

5. REAL TIME MESSAGING

5.1. OVERVIEW OF REAL TIME MESSAGING

Real time message processing requires an Internet Protocol transfer mechanism with a message management system, which is called a real time switch.

5.2. TCIB REAL TIME SWITCH WEB SERVICES: APPLICATION-LAYER PROTOCOL STACK

The API interaction with TCIB real time switch uses HTTP (Hypertext Transfer Protocol), as a text-base, application-layer protocol.

On the transport layer, HTTPS (Hypertext Transfer Protocol Secure) is technically used to transport the HTTP request and responses within a connection encrypted by TLS V1.1 (or later version). HTTPS helps prevent wiretapping and man-in-the-middle attacks by encrypting the entire HTTP transmission.

APPLICATION LEVEL SUITE PROTOCOLS USED

The following messages are used at the application layer of the protocol stack:

- HTTP POST request Posting data in the message payload
- HTTP 200 Ok Standard response for successful HTTP requests

The ISO 20022 XML message is encapsulated in the body of a HTTPS **POST** message. (HTTPS request carries the payload). This allows the ISO 20022 message to pass seamlessly over the public Internet. Details of ISO 20022 messages used are provided in sections below.

HTTP HEADER ELEMENTS

The following are the HTTPS header elements that will be included in both the request and response messages to and from the TCIB real time switch:

X-AUTH-USER-NAME	**E.G. Zanaco, ZB Bank Zimbabwe etc**
X-AUTH-USER-PWD	**b@nkse$v!23**
X-AUTH-API-VERSION	**ISO20022v1.0**
X-AUTH-CHECKSUM	**AJLF1341234**

The above HTTPS header must be contained in every request to the TCIB real time switch. (Likewise the TCIB real time switch will also contain these parameters to participants). BankservAfrica will allocate User Names and Passwords to participants on registration.

This header provides authentication between the participant and TCIB real time switch. The header also ensures that transmitting partners are using the agreed version of the API.

Authentication and checksums are not required for the Incubation Phase. The X-AUTH-CHECKSUM field may contain any character that will not be verified in the Incubation Phase.

5.3. ALLOCATION OF ENDPOINTS

All messages require endpoints to which they must be sent. Endpoint are Internet URLs or addresses. Each message type has to have an endpoint to complete message transfers.

The following is a template for defining endpoints:

https://<IP:PORT>/contextpath/

Note that all participants must define and share endpoints with BankservAfrica for receiving messages. Endpoints must be defined for

- Credit Transfers (Payments)
- Payment returns
- Status requests

In TCIB, endpoints are defined for participants sending messages to TCIB. The following endpoints are defined:

Payment API:

Method: HTTP POST

URL: https://uat-tcib.bankservafrica.com:23211/eig/payment

Body: ISO20022 pacs.008

PaymentReturn API:

Method: HTTP POST

URL: https://uat-tcib.bankservafrica.com:23211/eig/paymentreturn

Body: ISO20022 pacs.004

The above endpoint definitions include the message type associated with the endpoint and the HTTP command used for that endpoint.

Participants must configure similar endpoints.

In addition to setting up endpoints for payments and payment returns, an endpoint is configured for requesting the status of a message:

Status API:

Method: HTTP GET

URL: https://uat-tcib.bankservafrica.com:23211/eig/status/{MsgId}

The Status request is a HTTP GET command and must contain the message identifier <MsgId> being queried.

5.4. RULES FOR CREATING PAYLOADS OF MESSAGE PACKETS

Messages must contain HTTPS headers as detailed above.

The payload must be contain an ISO 20022 pacs.008 credit transfer message or an ISO 20022 pacs.004 payment return message as detailed in the section below and maintained on MyStandards.

The payload must commence with a definition of the version of XML being used and what encoding is used, as detailed below:

```
<?xml version="1.0" encoding="UTF-8"?>
```

ISO 20022 messages require a root tag, <Document>, to identify the version of the ISO 20022 message being carried. The following two root tags are defined for credit transfers and payment returns:

```
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:pacs.008.001.05"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Document xmlns="urn:iso:std:iso:20022:tech:xsd:pacs.004.001.05"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

The message must be terminated with a </Document> tag.

The payload of messages may only contain one transaction.

Messages must be one of the messages supported by the scheme.

The date in the message must be todays date, being the settlement date if the transfer is successful.

The payment must have the correct details regarding the sender and the beneficiary of the payment.

The sender must perform all validations as per as per the SADC TCIB Schema.

The TCIB Switch will perform validations as detailed in a section below.

5.5. PROCESSING CYCLES FOR TCIB REAL TIME SWITCH

The TCIB real time switch operates 24 X 7. These times are not for Incubation (Lean) phase.
The operating time for processing through TCIB for the Incubation (Lean) phase is 08H00 to 14H30.

At the end of a clearing window, a cutover is performed. Multiple clearing windows are catered for. This is not catered for in Incubation (Lean) phase.

At the end of a processing window, all "in-flight" (messages that are being processed, waiting for responses) messages are completed. During end of window cut-over, message/transaction logs are closed, stored and re-initiated for the next period.

At the end of the processing window, a "mark-off" file (transaction file) containing all the transaction sent and received are supplied to participants. The Mark-off file layout is given in Annexure 12.3.

Processing cycles by participants may be different to those of the real time switch. Participants are required to indicate the start of their processing window by sending Telnet "PING" messages. PING allows the sender to know whether a destination defined by an IP address is accessible via the internet, in this case the IP address of the production TCIB Real Time Switch. The real time switch will respond with PING messages to participants and keep a record of active participants.

After a configurable period (a parameter in the system that will be fine-tuned during testing, default value 1 minute), the TCIB switch will PING participants to see if they are still active on the network. The TCIB will retry sending the PING if a response is not received. The number of retries is configurable, and the default setting is 3 retries. If responses are not received from participants, participants will assumed to have closed their processing window.

5.6. CHECKING THE STATUS OF A MESSAGE

Unable to Connect to an Endpoint
If a sender is unable to connect to an endpoint, the sender must check that the VPN of the receiver is up. A Telnet "PING" can be used.

Status API
If sending partners do not receive responses from payment or payment return messages, the following request Status API may be send to request the status of the message processed:

Request:
Method: HTTP GET
URL Pattern: https://<IP:PORT>/contextpath/{**MsgId**}

The response should be

Response:

<response><code>{code}</code><message>{message}</message></response>

The status API for TCIB is

Method: HTTP GET

URL: https://uat-tcib.bankservafrica.com:23211/eig/status/{MsgId}

From a terminal emulator, the following (cURL) may be send from the command line to request the status of a message processed:

```
curl -k -vv \
-H 'X-AUTH-USER-NAME: [username]' \
-H 'X-AUTH-USER-PWD: [sha256 of plaintext password]' \
-H 'X-AUTH-API-VERSION: 1' \
-H 'X-AUTH-CHECKSUM: 123' \
https://uat-tcib.bankservafrica.com:23211/eig/status/{MsgId}
```

The Username and Password must be included and the Message Identifier (<MsgId>) of the ISO 20022 message must be included.

cURL stands for client URL. cURL tries to avoid handling the actual data that is transferred. It has, for example, no knowledge about HTML or anything else of the content that is popular to transfer over HTTP, but it knows all about how to transfer such data over HTTP.

The following is an example of a response to a Status request:

```
<response>
    <code>3000</code>
    <message>Success</message>
</response>
```

5.7. MESSAGE SCHEMA VERSIONS

The document is compatible with the following versions of messages

- pacs.008.001.05 ISO 20022
- pacs.004.001.05 ISO 20022
- HTTPS 200 response Network standard application protocol

5.8. MESSAGE STANDARDS

All messages must conform to message standards as detailed by international standards organization ISO 20022. Participants must have capability to create and receive the ISO 20022 TCIB messaging formats as per published XSDs. The XSDs are housed on SWIFT.com/Mystandards.

MYSTANDARDS PORTAL

SADC TCIB XSDs are documented in the SADC workspace on the SWIFT MyStandards http://www.swift.com/mystandards/.
For access to these standards, please contact Sharon Watt at sharonw@bankservafrica.com.
When access to MyStandards has been granted, refer to document **Logging into MyStandards** for directions on how to use the portal to obtain documentation and XSDs**.**

The SADC TCIB payment messages do not hold every detail of the full ISO 20022 messages and this is a "Light" version of the messages. Although light versions of the messages are used, the process flows supported by ISO 20022 are followed.

The message standards to be used for mobile payments are defined in the following documents:
*SADC_TCIB_FIToFICustomerCreditTransferV05 _**pacs.008.001.05***
*SADC_TCIB_PaymentReturnV05_**pacs.004.001.05***

Message templates with examples are included on MyStandards for downloading.

READINESS PORTAL AND HOW TO TEST

Participants can test messages against a test simulator called MyStandrds Readiness Portal. Detail on how to access the Readiness Port are provided in the document **Using the Readiness Portal on MyStandards.**

5.9. CHARACTER SET

The character set for credit transfers allows for both upper- and lower-case alphabetic characters.

The allowable character set is defined as follows:

A – Z	ALPHABETIC	+	PLUS
0 – 9	NUMERIC	$	DOLLAR
.	PERIOD	;	SEMI-COLON
-	HYPHEN	=	EQUAL
*	ASTERISK	@	AT
,	COMMA	?	QUESTION MARK
(	LEFT PARENTHESIS	:	COLON
)	RIGHT PARENTHESIS	~	TILDA
	SPACE		
%	PERCENTAGE		

Originators of TCIB payment and return messages must comply with the characters set above.

5.10. ISO 20022 MESSAGE IDENTIFIERS AND TRANSACTION IDENTIFIERS

ISO 20022 messages are identified by the Message Identifier <MsgId> and transactions are identified by End-to-End Identifier <EndToEndId> and Transaction Identifier <TxId>.

The TCIB system requires unique Message Identifiers and Transaction Identifiers.

The following elements are to be included in Message identifiers and Transaction Identifiers to ensure uniqueness:

Date in format CCYYMMDD	8 digits
Scheme Participant Identifier (SPID)	6 digits (your own SPID)
Message or transaction reference	no restriction, any identifier that has meaning to your business

The following are examples of message identifiers and transaction identifiers adhering to the above rules:

<MsgId>20190701290000168953645</MsgId>
<EndToEndId>20190701290001KGB57799</EndToEndId>
<TxId>20190701290001KGB57799</TxId>

Note that the EndToEnd Transaction Id and the Transaction Id may contain the same values.

5.11. HTTP 200 RESPONSE

All API calls to the TCIB Real Time switch are acknowledged with a HTTP200 OK XML response message:

1) The follow construct is used for a positive response

```
<response>
        <code>3000</code>
        <message>Success</message>
</response>
```

2) The following construct is used for a negative response

```
<response>
        <code>xxxx</code>
        <message>Failure</message>
</response>
```

The list of error codes are supplied in annexure 12.2.

5.12. RESPONSE FROM PARTICIPANTS

Participants receiving messages from the TCIB real time switch must respond with an HTTP200 OK XML response message:

2) If the payload message passes validation and is applied successfully to the destination account, the response should be:

```
<?xml version="1.0" encoding="UTF-8"?>
        <response>
                <code>3000</code>
                <message>Success</message>
        </response>
```

3) If the payload message fails validation or cannot be applied at the destination participant, the response should be:

```
<?xml version="1.0" encoding="UTF-8"?>
        <response>
                <code>xxxx</code>
                <message>message</message>
        </response>
```

A list of error codes are supplied in annexure 12.2. The most common error code to be used is **REMIT FAILED** error code **3032**.

5.13. DATE AND TIME

All Date and time elements in messages must be in CAT.

5.14. REGULATORY REQUIREMENT FOR MESSAGE CONTENT

For all SADC mobile to mobile transactions the mobile phone number is required, but can be accommodated (due to regulatory requirements) by the name and postal Address.

If the mobile number is not provided then at least name is mandatory.

The inclusion of the address depends on the country regulatory.

5.15. VALIDATIONS PERFORMED ON REAL TIME MESSAGES

All messages submitted to the TCIB Real Time Switch are validated before processing.
The structure of the message is checked against the published XSD on MyStandards.
The following additional validations occur within the TCIB Real Time Switch.

SOURCE OF MESSAGE IS AUTHENTICATED

The originator of the message is authenticated by referencing the authentication component in the header.
Error: 1003 Authentication failed.

INCORRECT IP ADDRESS

The IP Address is incorrect.
Error: 1008 Authentication failed.

SOURCE CURRENCY INCORRECT

The currency of the amount of the transaction is not a valid currency loaded on the system
Error: 1012 Currency does not exist.

INCORRECT SOURCE IDENTIFIER

The SPID or BIC code of the originator is not loaded on the system
Error: 1017 Source participant invalid.

INCORRECT DESTINATION IDENTIFIER

The SPID or BIC code of the destination is not loaded on the system
Error: 1018 destination participant invalid

CORRIDOR FAILURE

Transactions in the corridor between two transacting participants outside the activation dates for the corridor on the system.
Error: 1023 Corridor validation failed

INVALID DATE TIME

The date and time in the transaction is invalid
Error: 3001 Invalid date/time

USER SENDING LIMIT REACHED

The agreed sending item limit has been exceeded

Error: 3077 User Sending Limit exceeded

PARTNER RECEIVING LIMIT REACHED

The agreed receiving item limit has been exceeded

Error: 3078 User Sending Limit exceeded

PARTNER SENDING LIMIT REACHED

The agreed aggregate sending amount limit has been exceeded

Error: 3075 Partner Sending Limit exceeded

PARTNER RECEIVING LIMIT REACHED

The agreed aggregate receiving amount limit has been exceeded

Error: 3076 Partner Sending Limit exceeded

6. MESSAGE MANAGEMENT CAPABILITIES OF TCIB

The real time TCIB Real Time switch supports complete message management. TCIB Real Time switch handles message time outs and checks for duplicate messages.

The following functionality is handled by TCIB Real Time switch

- Ensuring that communication channels are open and active
- Date changes at cut over processing
- Message delivery time outs
- Duplicate checking of messages received
- Message content validation
- Item limit checking.

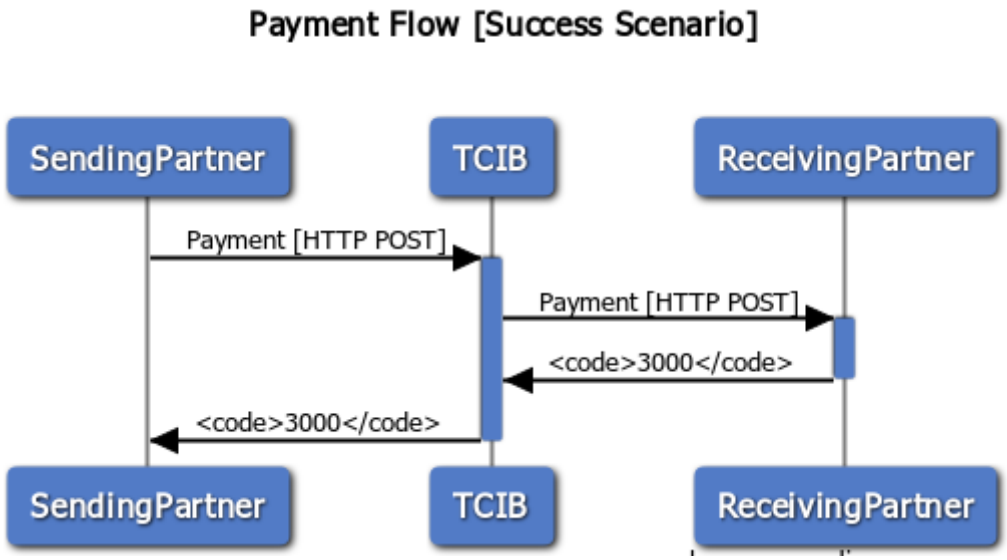
6.1. MESSAGE FLOWS SUPPORTED

The TCIB Real Time switch has the capability of processing the following business messages:

- Bank to Bank
- Non-bank (mobile) to Bank
- Bank to non-bank (mobile)
- Non-bank(Mobile) to non-bank (mobile)
- Bank(mobile) to non-bank (mobile)
- Bank(mobile) to non-bank
- Cash to bank
- Bank to cash
- Cash to mobile
- Mobile to cash
- Cash to cash

6.2. SUCCESSFUL PAYMENT FLOW

The following diagram show the message flow for a successful payment.



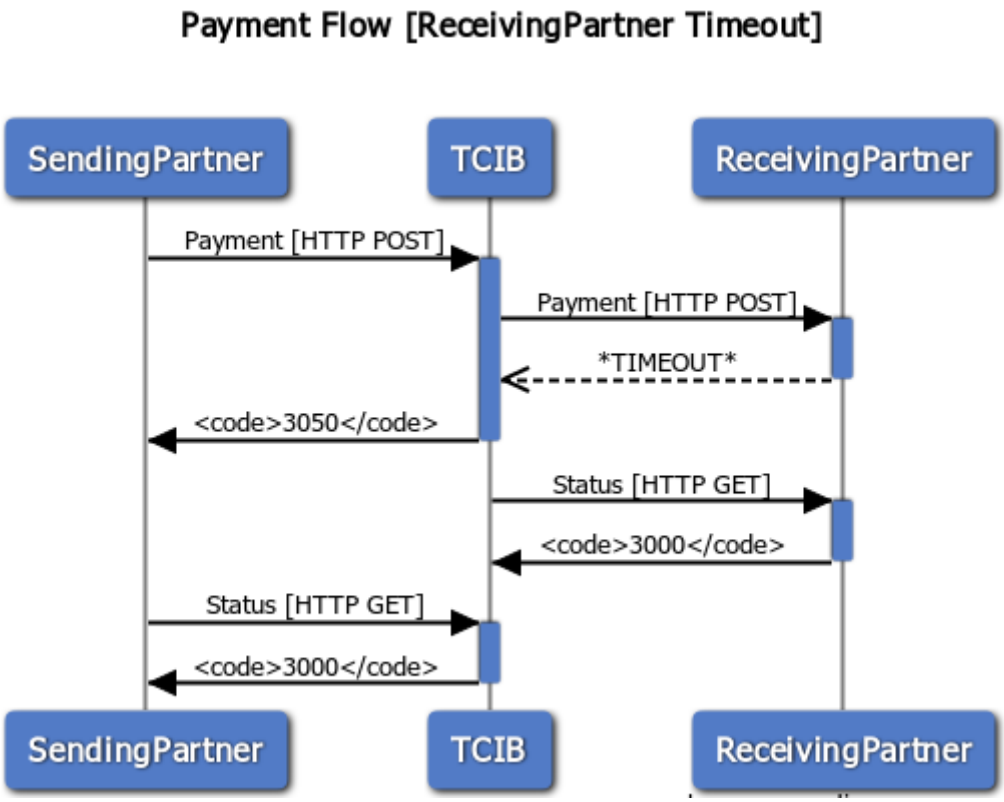
1) A credit transfer (or payment return) is included in the payload of an HTTP POST message.
2) The message is sent to the payment endpoint as supplied by BankservAfrica.
3) TCIB will validate the message and if the message is successful, it will be sent to the receiving partner's endpoint.
4) If the message passes validation at the recipient and the payment can be applied, the receiving partner must construct a HTTP 200 "successful" response and send it to the TCIB endpoint.

The response format is same for payment and payment returns and is supplied below:

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
    <code>3000</code>
    <message>Success</message>
</response>
```

6.3. PAYMENT FLOW: RECEIVING PARTNER TIMES OUT

A “Timeout” is when a message is sent and a response has not been received within the agreed time. This payment flow must be followed when a message is sent to a receiver and a reply is not received by TCIB.



1) A payment (or payment return) is included in the payload of an HTTP POST message.
2) The message is sent to the TCIB payment (or payment return) endpoint as supplied by BankservAfrica.
3) TCIB will validate the message and if the message is successful, it will be sent to the receiving partner’s endpoint. TCIB starts a timer.
4) If the timer reaches the agreed timeout period (initially 30 seconds), TCIB sends a HTTP 200 “timeout” message to the sending partner. The construct of the timeout message is given below

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
        <code>3050</code>
        <message> Transaction Pending</message>
</response>
```

The **<code>3050</code>** represents transaction is pending and is not the final status

5) TCIB will send a HTTP GET Status request message to Receiver Partner.

6) In this example, the receiving partner sends a HTTP 200 positive response.

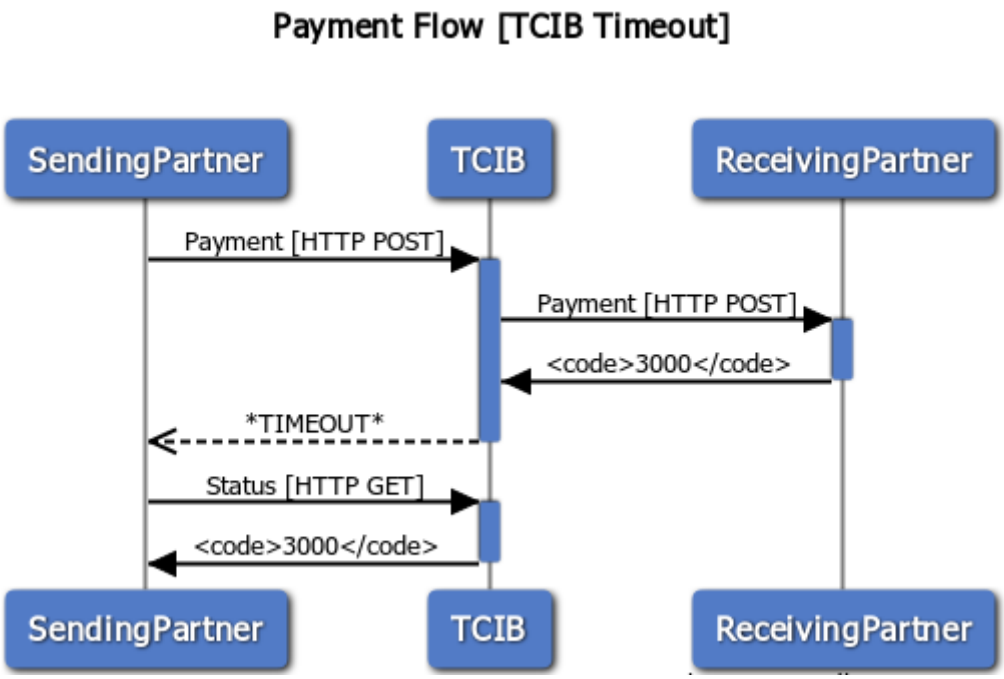
```
<?xml version="1.0" encoding="UTF-8"?>
<response>
    <code>3000</code>
    <message>success</message>
</response>
```

7) Sending Partner will send HTTP GET Status requests to TCIB continuously after parameterised time interval until they get final status. (i.e, until they get code other than 3050).

8) TCIB sends the HTTP 200 positive response to the sending partner.

6.4. PAYMENT FLOW: TCIB TIMES OUT

This payment flow must be followed when a message is sent to TCIB and a reply is not received from TCIB within an agreed time.



1) A payment (or payment return) is included in the payload of an HTTP POST message.
2) The sending partner sends the message to the TCIB payment (or payment return) endpoint as supplied by BankservAfrica. The sending starts a timer.
3) TCIB validates and sends the message to the receiving partner.
4) The receiving partner sends an HTTP 200 successful response to TCIB.
5) After an agreed time, the sending participant has not received the HTTP 200 successful response.
6) The sending partner sends an HTTP GET status request to TCIB.
7) TCIB responds with an HTTP 200 successful response.

7. EXCEPTION PROCESSING AND PROCESS FLOWS

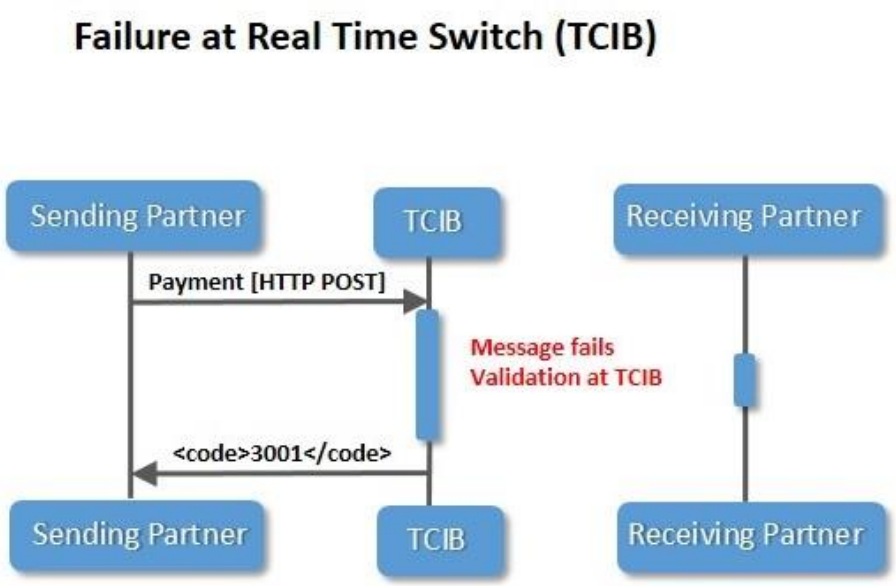
There are a number of situations where the processing of credit transfers cannot be concluded due to exception conditions. Such exception conditions includes

- Validation failures at TCIB
- Validation failure at destination participant
- Payment returns
- Message authentication failure
- Financial limits exceeded

This section details such exception processes.

7.1. FAILURE AT RCSO REAL TIME SWITCH

The RCSO Real Time switch validates input from participants. Should a message fail validation, the following process flow is followed:



The following message flows occur when a message fails at the Real Time Switch:

- A sender requests a bank/non-bank to send a credit transfer to a bank account/wallet/cash pay-out point.
- The bank/non-bank initiates a HTTPS POST message with a payload containing ISO 20022 credit transfer message to RCSO system.
- RCSO system validates the message and one or more elements fails in validation.
- RCSO returns a HTTP 200 NACK XML messages containing an error code to the originator.

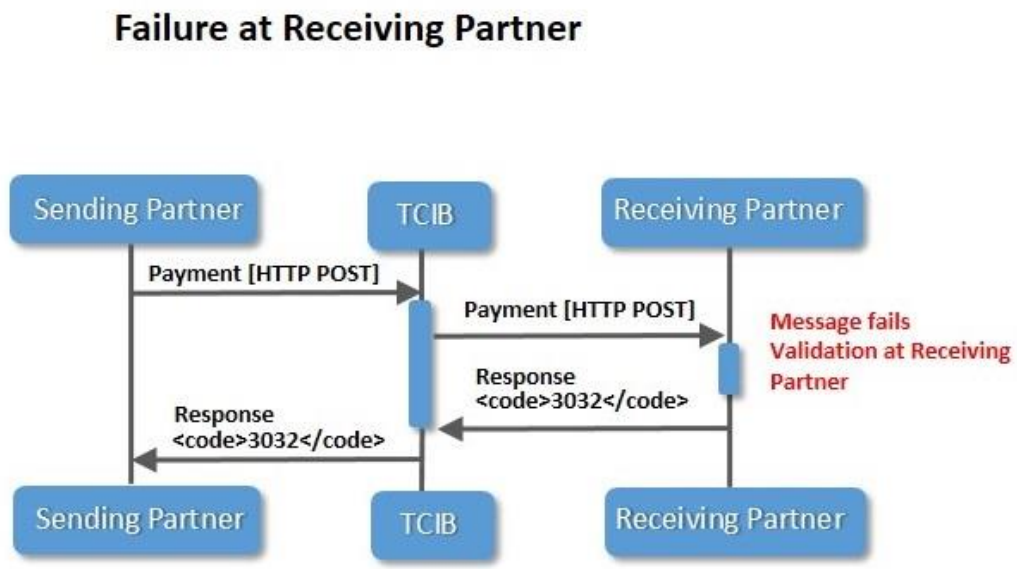
The following is an XML message returned for a message with an invalid date and time:

```
<response>
   <code>3001</code>
   <message>Failure</message>
</message>
```

Error codes are contained in Annexure 12.2.

7.2. FAILURE AT DESTINATION PARTICIPANT

The receiving participant validates input from TCIB. Should a message fail validation or cannot be applied to a destination account, the following process flow is followed:



The following message flows occur when a message fails at destination participant

- A sender requests a bank/non-bank to send a credit transfer to a bank account/wallet/cash pay-out point.
- The bank/non-bank initiates a HTTPS POST message with a payload containing ISO 20022 credit transfer message to RCSO system.
- RCSO system validates the message and sends the message to the destination participant.
- The message fails at the destination participant.
- The destination participant creates an HTTP 200 NACK XML messages containing an error code to the originator.
- The failed response message is sent to TCIB.
- TCIB sends the failed response message to the sending participant.

The following is an XML message returned for a message with a remittance failure:

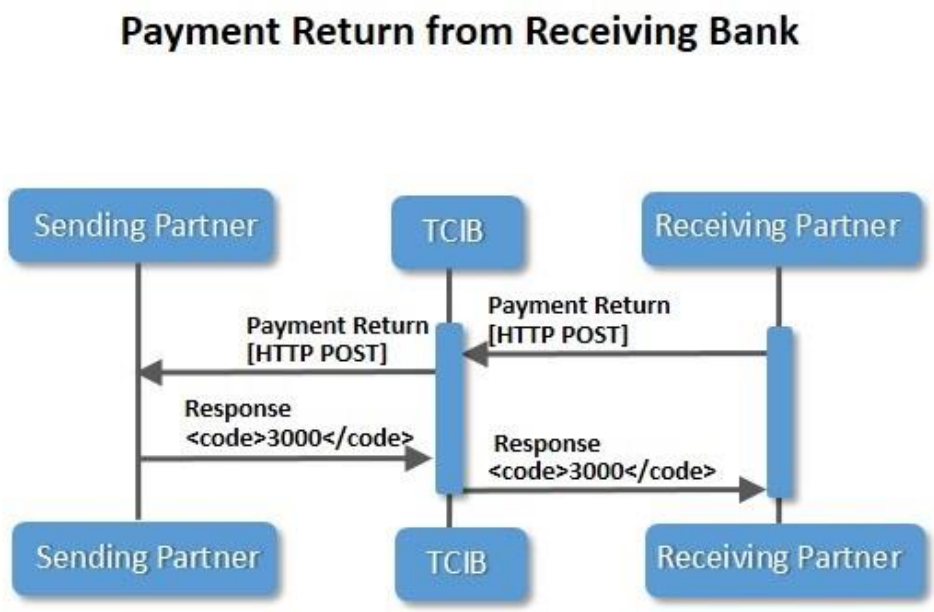
```
<message>
  <code>3032</code>
  <message>Remit Failed</message>
</message>
```

Error codes are contained in Annexure 12.2.

7.3. PAYMENT RETURNS

When a credit transfer is delivered to a participant and acknowledged with a HTTP 200 success message, the payment is considered complete and settlement takes place between the two sponsoring banks.

If, for any reason, the payment cannot be credited to the beneficiary, or the payment is duplicated, the beneficiary participant must use a pacs.004 payment return to reverse the original payment. The diagram below shows the process flow for a payment return.



A previous credit transfer has been performed successfully and settled between a sending (debtor) participant and a receiving (creditor) participant in another country.

The following message flows occur when a message fails at the creditor participant:

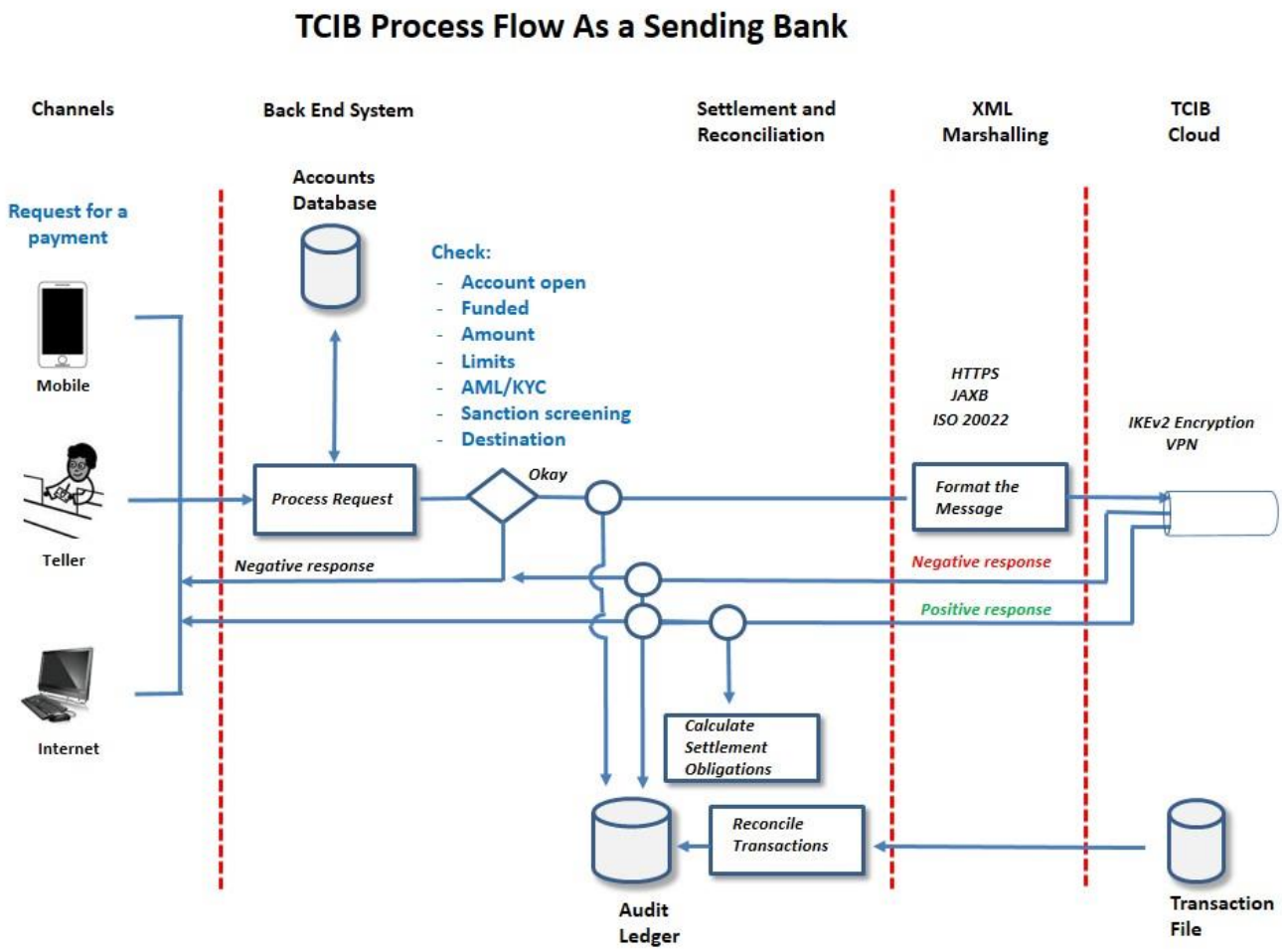
- For whatever reason, the creditor participant is required to return a previously made payment. The creditor participant initiates a HTTPS POST message with a payload containing ISO 20022 payment return message to RCSO system.
- RCSO system forwards the HTTPS POST message with a payload containing ISO 20022 payment return message to the originating debtor participant, and the originating participant account is credited.
- The originating debtor participant acknowledges the payment return message by sending a HTTP 200 XML message containing a success code 3000 to the TCIB Real Time switch.
- TCIB Real Time switch send the HTTP 200 XML messages containing a success code 3000 to the receiving bank.

The reason for returning the credit transfer is contained in the Return Reason Code Appendix 12.4

8. DIAGRAMS OF TCIB INTEGRATION TO PARTICIPANT SYSTEMS

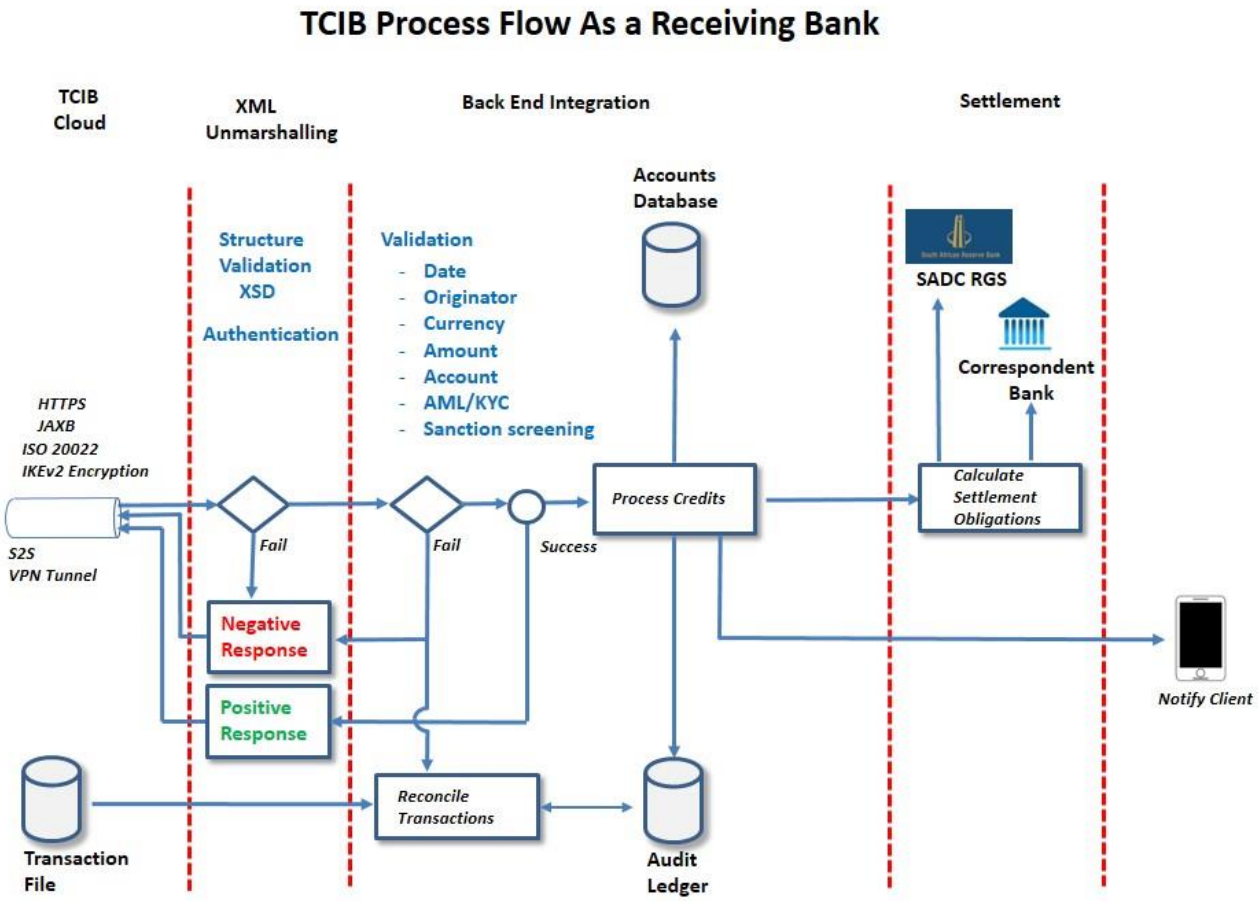
The following paragraphs provide integration diagrams for banks and participants for sending and receiving payments and payment returns.

8.1. TCIB PROCESS FLOW AS A SENDING BANK



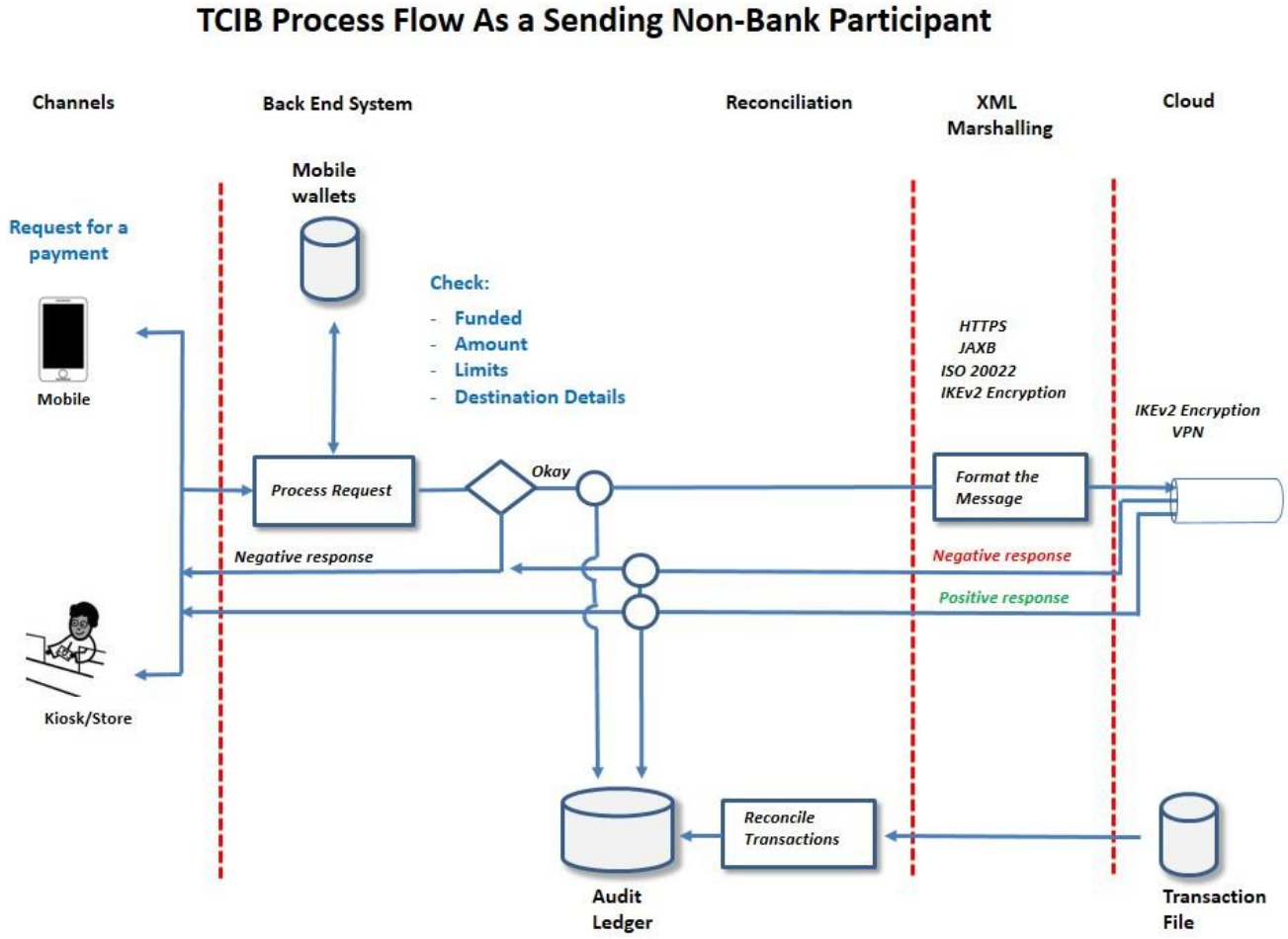
The above diagram depicts a schematic process flow for a bank initiating a payment or a payment return. Note the reconciliation process reconciles positive (successful) and negative (unsuccessful) responses to TCIB transaction file at end of clearing window.

8.2. TCIB PROCESS FLOW AS A RECEIVING BANK



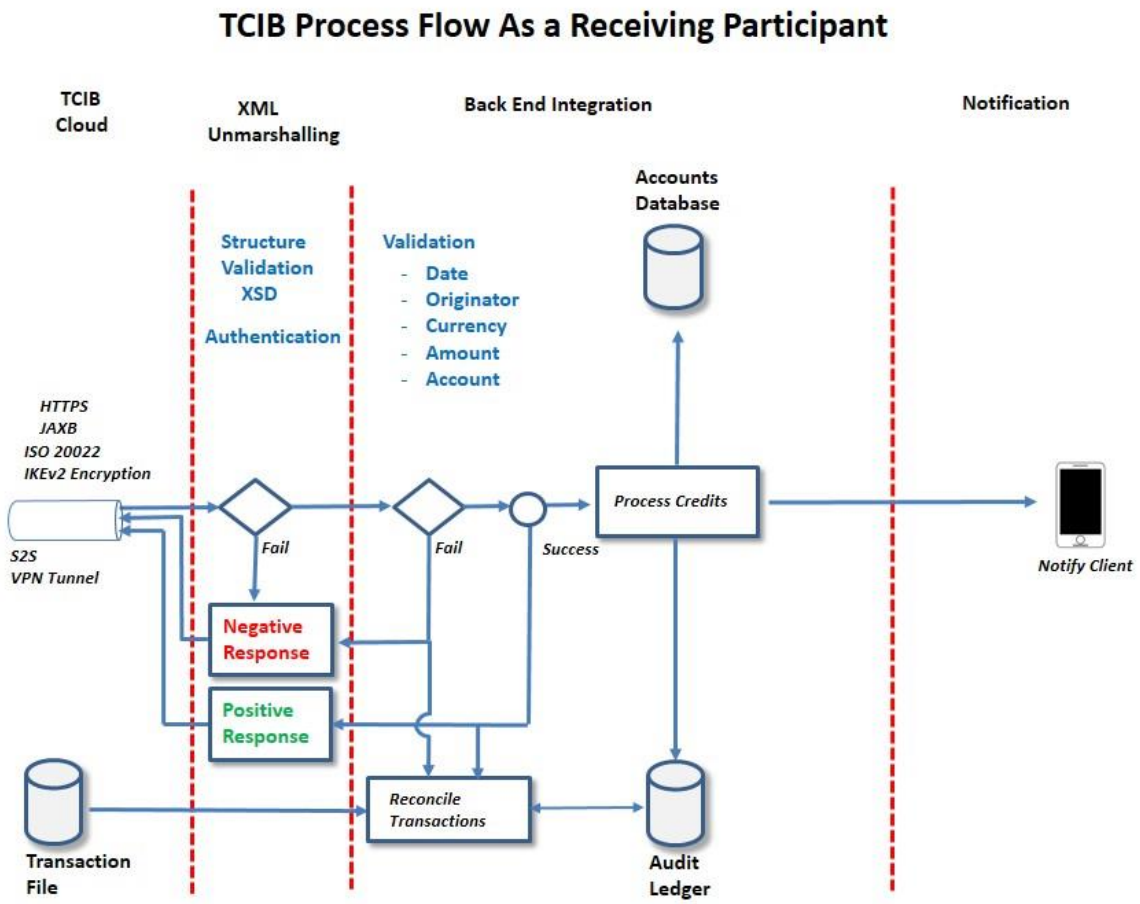
The above diagram depicts a schematic process flow for a bank receiving a payment or a payment return. Note the validation requirements and how successful transactions are applied to settlement for reconciliation with TCIB at end of clearing window. Also note that positive and negative responses are reconciled against the TCIB transaction file at the end of clearing window.

8.3. TCIB PROCESS FLOW AS A SENDING PARTICIPANT



The above diagram depicts a schematic process flow for a participant initiating a payment or a payment return. Note the positive (successful) and negative (unsuccessful) responses are recorded for reconciliation with the TCIB transaction file at end of clearing window.

8.4. TCIB PROCESS FLOW AS A RECEIVING PARTICIPANT



The above diagram depicts a schematic process flow for a participant receiving a payment or a payment return. Note the validation requirements and reconciliation with TCIB transaction file at end of clearing window.

9. CHANGE REQUESTS

Should a participant have a requirement for exception processing that requires the use of additional ISO 20022 messages, these requirements must be submitted as a formal request to BankservAfrica as detailed in the TCIB Change Request Process manual. Change requests must be completed and sent to your country's project coordinator. Approved change requests are sent by the project coordinator to the Payment System Management Body. The Payment System Management Body will evaluate the change request and approve the change request. The change request will be sent to participating banks and the RCSO.

10. SETTLEMENT PROCESSING

Amounts, originating and destination identifiers contained in messages are used to calculate settlement obligations of banks to other banks participating in TCIB processing.

For settlement processing, refer to **TCIB Settlement Procedure** manual.

11. ANNEXURES

11.1. MASTER DATA MANAGEMENT INFORMATION

Details of Master Data held for processing by RCSO is published in TCIB Master Data Management document. The table below provides a participant static details held on the Master Data Management repository.

Element Name	Element Description
MDM Record Type	Identifies the MDM data record type (where 44 = Participant Static, Shared Detail Record)
TCIB Participant Name	Registered Name of the TCIB Participant
Activation Status	Active / Inactive / Test (A or I or T)
Country Code	Registered Country Code (ISO Standard)
Created On	Date when created / loaded (format yyyy/mm/dd)
Created By	Created by whom
Modified On	Date when modified (format yyyy/mm/dd)
Modified By	Modified by whom
TimeZone	CAT
Validity From	Date in format yyyy/mm/dd
Validity To	Date in fomat yyyy/mm/dd
Suspension From	Date in format yyyy/mm/dd
Suspension To	Date in fomat yyyy/mm/dd
Participant Type	Participant Bank / MNO / Remit Operator / Retailer / MMSP / PPSP / Mobile Switch / ADLA / Hub
Participant Short Code	2 Character Short Code (for data delivery)
Participant Short Name	Short Unique Name (for use in reports and alerts)
Participant SPID	Scheme Payment Identification code (as allocated by BSA - for all participants i.e. Banks / non-Banks)
Participant SWIFT BIC Code (PROD)	Production SWIFT BIC Code if participant is a Bank (else use RCSO unique SPID code for participant)
Participant SWIFT BIC Code (TEST)	Test SWIFT BIC Code if participant is a Bank (else use RCSO unique SPID code for participant)
Participant Hub SPID	SPID of Hub if processed via a hub else it will contain its own SPID
Settlement Officer Name	Person responsible for settlement
Settlement Email Address	Email address for settlement related emails
Settlement Officer Phone Number	Office phone number of settlement officer
Settlement Officer Mobile Number	Mobile number of settlement officer
Business Owner Name	Person responsible for TCIB payments
Business Owner Email Address	Email address for Person responsible for TCIB payments
Business Owner Phone Number	Office phone number of person responsible for TCIB payments

Business Owner Mobile Number	Mobile number of person responsible for TCIB payments
Billing Contact Name	Name of Contact person for billing
Billing email address	Email for billing
Billing Mobile Number	Billing contact mobile number
Product Support Name	Contact person for production issues
Product Support Email Address	Email address for contact person for production issues
Product Support Phone Number	Office phone number of contact person for production issues
Product Support Mobile Number	Mobile number of contact person for production issues

The table below provides a participant details by currency held on the Master Data Management repository.

Element Name	**Element Description**
MDM Record Type	Identifies the MDM data record type (where 45 = Participant Detail Record by Currency)
Participant SPID	Scheme Payment Identification code (as allocated by BSA - for all participants i.e. Banks / non-Banks)
Currency	Currency - ISO Standard (i.e. ZAR, USD, ZMW)
Currency Item Limit	Currency Item Limit (I.e. Max ZAR 2,000 / USD 180 / ZWM 1,800)
Settlement Bank for this Currency	Settlement Bank - Short Unique Name (for use in reports and alerts)
Bank SWIFT BIC Code of the participant's Settlement Bank (PROD)	Production SWIFT BIC Code of the Settlement Bank for this currency's settlement
Bank SWIFT BIC Code of the participant's Settlement Bank (TEST)	Test SWIFT BIC Code of the Settlement Bank for this currency's settlement
RTGS SWIFT BIC Code for Currency to settle in (PROD)	Production SWIFT BIC Code of the RTGS for this currency's settlement
RTGS SWIFT BIC Code for Currency to settle in (TEST)	Test SWIFT BIC Code of the RTGS for this currency's settlement
Settlement exposure limit for Currency	(I.e. Max ZAR 1,000,000 / USD 180,000 / ZWM 1,800,000)

For more information about TCIB data management system, kindly refer to TCIB Master Data Management document.

11.2. RCSO ERROR RESPONSE MESSAGES

The following error responses will be returned when a payment or payment return fails at the Real Time switch:

Error Code	Short Description	Detailed Description
1003	AUTHENTICATION FAILED	Failure - Authentication Failed (Authentication component in message header incorrect)
1007	FAILURE UNKNOWN REASON	Failure - Reason Unknown (various possible reasons)
1008	IP UNAUTHORIZED	Failure - Unauthorised IP Access (incorrect URL used)
1009	SYSTEM RESPONSE ERROR	Failure - System Error (various possible reasons)
1012	SRC CURRENCY NOT EXIST	Failure - Invalid source (originating) currency (currency in payment used by sending institution not registered on the system)
1013	DEST CURRENCY NOT EXIST	Failure - Invalid destination (final) currency (currency used in the payment of the destination country not registered on the system)
1017	SRC PARTNER VALIDITY FAIL	Failure – Invalid source (originating) partner (originating financial institution not registered on the system)
1018	DEST PARTNER VALIDITY FAIL	Failure – Invalid destination (final) partner (receiving end financial institution not registered on the system)
1019	SRC PARTNER SUSPENDED	Failure - Source (originating) partner suspended (transfers of originating financial institution suspended)
1020	DEST PARTNER SUSPENDED	Failure – Destination (final) partner suspended (end receiving financial institution transfers suspended)
1021	SRC PARTNER INACTIVE	Failure - Source (originating) partner not active (sending financial institution not activated on the system)
1022	DEST PARTNER INACTIVE	Failure – Destination (final) partner not active (receiving end financial institution not activated on the system)
1023	CORRIDOR VALIDITY FAIL	Failure –(transactions in the corridor between two transacting financial institutions outside the activation dates for the corridor on the system)
1024	CORRIDOR SUSPENDED	Failure –Transactions between the two countries in the payment message have been suspended
1025	CORRIDOR INACTIVE	Failure –Corridor has not been activated on the system
1026	SRC MSISDN NOT ALLOWED	Failure –Mobile phone number used by sending financial institution not allowed
1027	SRC MSISDN BLACKLISTED	Failure – Mobile phone number used by sending financial institution has been blacklisted)
1028	DEST MSISDN NOT ALLOWED	Failure – Receiving mobile number not allowed to receive transfers
1029	DEST MSISDN BLACKLISTED	Failure – Receiving mobile number blacklisted
1030	CORRIDOR NOT EXIST	Failure – Corridor has not been set up yet on the system
1031	SRC CURRENCY INACTIVE	Failure - Invalid source (originating) currency (currency of sending financial institution not activated on the system)
1032	DEST CURRENCY INACTIVE	Failure - Invalid destination (final) currency (currency of destination country not activated on the system)
1046	MESSAGE ID NOT FOUND	Failure to match the Message ID in status message to messages received.

Error Code	Short Description	Detailed Description
1079	SRC PARTNER INVALID	Failure – Invalid source (originating) partner (Sending financial institution transacting outside of the activation dates set for their activity on the system – i.e. valid from – valid until)
1080	DEST PARTNER INVALID	Failure – Invalid destination (final) partner (receiving financial institution transacting outside of the activation dates set for their activity on the system – i.e. valid from – valid until)
1081	SRC MSISDN INVALID	Failure – Mobile number in message of sending financial institution not a valid number
1082	DEST MSISDN INVALID	Failure – Mobile number of recipients of funds not valid
1599	MESSAGE TIMEOUT	Failure – The time from transmission of a message to receipt of a response has exceeded the acceptable limit.
1600	DESTINATION PARTICIPANT IS DOWN	Failure – destination participant is down
3000	SUCCESS	Success - Transaction processed successfully
3001	INVALID DATE/TIME	Failure – Date / time not valid
3004	DUPLICATE TRANSACTION ID	Failure – Transaction ID is a duplicate (Sender to check to to if transfer has been duplicated)
3032	REMIT FAILED	Failure – Remittance failed (transfer rejected for various reasons)
3050	TRANSACTION PENDING	Transaction pending, not in final status
3075	PARTNER SENDING LIMIT REACHED	Failure – Sending partner limit exceeded (Limit for the sending participant financial institution reached)
3076	PARTNER RECEIVING LIMIT REACHED	Failure – Receiving partner limit exceeded (Limit for the receiving participants financial institution reached)
3077	USER SENDING LIMIT REACHED	Failure – Sending user limit exceeded (Limit of sender client provided by the sending financial institution reached)
3078	USER RECEIVER LIMIT REACHED	Failure – Receiving user limit exceeded (Limit of receiving client of receiving financial institution reached)

11.3. MARK-OFF FILE LAYOUT

Details of mark-off file are given below

File specifications:

Data Structure:	Comma delimited.	
File Name Structure:	*Date*D_TR_SPID.csv	Example **20190218D_TR_270001.csv**

Header Record

Element	*Contents*	*Comments*
Type	Daily Transaction Report	
Partner Name	ZB Bank	
Id	TZB20190219070001291941	
Start Time	2019-02-18 00:00:00	Time given in CAT
End Time	2019-02-18 23:59:59	
Generated Time	2019-02-19 07:00:01	
Timezone	CAT	

Transaction Record

Element	*Contents*	*Comments*
Received Time	15-02-2019 14:15	
Last Update Time	18-02-2019 07:56	
EndToEndId	186837829	
Status	Remit Success	See statuses below
Type	DR	This is a debit to the bank
Source Partner	290001	SPID of source
Src Settlement Bank	290001	SPID of Source Settling Bank
Source Country	ZW	
Destination Country	ZA	
Destination Amount	496260	
Destination Currency	ZAR	
Destination Partner	214001	SPID of Destination Partner
Dest Settlement Bank	210004	SPID of Destination Settling Bank
Transaction Id	TPZB000001690981	Internal TCIB transaction id
Sender MSISDN	+9711082468	Sender's mobile Number
Sender Name	DRAKE MITI	
Receiver MSISDN	+9711082468	Receiver's mobile Number
Receivers Name	ALDE MAURRICE	
Transaction Type	WALLET	See Transaction Types below

Trailer Record

Element	*Contents*	*Comments*
Total Records	4	

The following table provides contents that can be expected in the Status and Transaction Type elements:

Status Table

STATUS	DESCRIPTION
Remit Success	Successful Transaction, applied to settlement
Bank Credit Failed	Failed Transaction, not applied to settlement

Transaction Table

TRANSACTION TYPE	DESCRIPTION
WALLET	Mobile Wallet
BANK	Bank Account
CASH	Cash Transfer

11.4. PAYMENT RETURN CODE

The following ISO payment return codes are used in payment return messages processed by TCIB:

RETURN CODE	DESCRIPTION
AM02	Not Allowed Amount
AM05	Duplication
BE06	Unknown End Customer
CNOR	Creditor MNO Not Registered
CUST	Requested By Customer
DNOR	Debtor MNO Not Registered
MD06	Refund Request By End Customer
RR02	Missing Debtor Name And Mobile Number
RR03	Missing Creditor Name And Mobile Number
RR04	Regulatory Reason
AC01	Incorrect Account Number
AC04	Closed Account Number
AC06	Blocked Account
AG01	Transaction Forbidden
AG02	Invalid Bank Operation Code
AM01	Zero Amount
AM03	Not Allowed Currency
AM06	Too Low Amount
AM07	Blocked Amount
AM09	Wrong Amount
BE01	Inconsistent With End Customer
BE04	Missing Creditor Address
BE05	Unrecognised Initiating Party
BE07	Missing Debtor Address
DT01	Invalid Date
MS03	Not Specified Reason Agent Generated
ED01	Correspondent Bank Not Possible
ED03	Balance Info Request
MD07	End Customer Deceased
MS02	Not Specified Reason Customer Generated
RC01	Bank Identifier Incorrect
RF01	Not Unique Transaction Reference
TM01	Cut Off Time
ED05	Settlement Failed
AM10	Invalid Control Sum