MT 103 – MX PACS.008

FORMAT CONVERTER

<Software Requirement Specification>

Date: <16/09/2022>

Table of Content

CROSS BORDER CREDIT TRANSFER

1. Identification of Team:

Vatsal Sinha 2020BCS0012

Yogesh Raj 2020BCS0076

Zishan Ahmad 2020BCS0078

Sagar Raj 2020BCS0156

2. Introduction

The introduction of the Software Requirements Specification (SRS) provides an overview of the entire SRS with purpose, scope, definitions, acronyms, abbreviations, references and overview of the SRS.

2.1. Purpose

The purpose of the document is to state and define different APIs working description for MT103 file to MX PACS.008 file conversion according to international norms and laws, specifically for cross border credit transitions.

2.2. Scope

This product targets International Bank, State Bank, Government Regulated Banking Authority <Features are not accessible for General People>.

2.3. Overview

The input message from credit sender is taken into the system in SWIFT MT message format from a file directory endpoint or a rest endpoint. Message can be received in BULK. After receiving the message, processing on this input text is done. In processing, input message shall be structurally verified as SWIFT MT message. Input message content shall be semantically verified against a stimulated core banking service, all messages with errors shall be deposited in a

DLQ (Dead Letter Queue). After processing the MT 103 format input is transformed into the MX PACS.008 format, output will pass through different message integration endpoints. Final output will be in MX PACS.008 message format.

3. Overall Description

- The user will upload the MT 103 file request in the Upload API from where the file will be uploaded in the local uploads file directory through a middleware. An upload message will be displayed.
- Then the user can verify this MT file by making the verification request in the Verification API. The verification is done in all levels: Application Header, Basic Header Validation, Block Breaker (sections of MT file input format), Text Header, User Header and Trailer Header. The validation is done on basis of the length of the message and the parenthesis checking along with reading of the instructed tags of control. If the validation fails the appropriate message will be displayed to the user.
- After the validation of the MT file format the user can request for the MT to MX file conversion and the current file will be converted to the XML format using the MT to MX conversion logic. (In the getMX function API). <<The conversion rules are predefined>>.
- This MX file is returned to the user at the requested Endpoint for completing the transaction request.

4. Specific Requirements

4.1. Functionalities

1. BASIC HEADER: The only mandatory block is the basic header. The basic header contains the general information that identifies the message, and some additional control information about the transaction process. The FIN interface automatically builds the basic header.

2. APPLICATION HEADER: The application header contains information that is specific to the application in use. The application header is required for messages that the users or the system and users, exchange. Exceptions are session establishment and session closure.

3. USER HEADER: The user header is an optional header. It consists of small details like the time and date of the generation of the transaction request and the Message Input Reference address (of the device), Banking Priority flags and check flags. NOTE: The User Header is not a mandatory field which means it is not always available until and unless the transaction method requests for it in specific transactional requests.

4. TEXT: The text is the actual data related to the transfer. It contains the transaction id and the account connection addresses along with the amount to be transferred and the valid format file of the transaction.

5. TRAILERS: The trailer either indicates special circumstances like return message and resending details and code which is relate to message handling. It also contains security information like the checksum of the message for error detection at the receivers end and the message authentication code (MAC value).

4.2. Security

4.2.1. Data Transfer

The system shall use secure sockets in all transactions that include any confidential customer information.

The system shall terminate automatically log out all customers after a period of inactivity. The system shall confirm all transactions with the customer's web browser. The system shall not leave any cookies on the customer's computer containing the user's password. The system shall not leave any cookies on the customer's computer containing any of the user's confidential information.

4.2.2. Data Storage

The customer's web browser shall never display a customer's password. It shall always be echoed with special characters representing typed characters. The customer's web browser shall never display a customer's credit card number after retrieving from the database. It shall always be shown with just the last 4 digits of the credit card number. The system's back-end servers shall never display a customer's password. The customer's password may be reset but never shown. The system's back-end servers shall only be accessible to authenticated administrators. The system's back-end databases shall be encrypted.

4.3. Communication Interface

The MT/MX converter shall use the HTTP protocol for communication over the internet and for the intranet communication will be through TCP/IP protocol suite.

4.4. Licencing Requirement

Not Applicable.

4.5. Applicable Standards

It shall be as per the industry standard.

5. Supporting Information

1. Cost --- No additional cost in implementation and setup, in fact it reduces load and cost of the server and infrastructure, it is also easier to process which reduces the cost of dedicated servers for time stamped transactions as they can now be easily processed on the normal server with normal processing power.
2. Flexibility --- APIs and the Micro-Service Structure provides room for updating and scalability in separate features but no flexibility is provided in the processing methods which are confined within the allowed laws.
3. Constraints --- MT 103 file only, HTTP Protocol for Communication over the Internet, File format and transaction type request should match the international laws and norms.