Discovery Report

Volume 2. WAY4 SOA API for ePIN

Orient Commercial Bank

Version 1.0

Status: Final

Date: 11.08.2020

Prepared by: OpenWay

Author: Tu B. Nguyen

Approved By: Tu B. Nguyen

1. Table of Contents

[1. Table of Contents 2](#_Toc49176266)

[2. History of changes 3](#_Toc49176267)

[3. Introduction 4](#_Toc49176268)

[3.1. Notations 4](#_Toc49176269)

[4. Introduction 5](#_Toc49176270)

[4.1. Overview 5](#_Toc49176271)

[4.2. API List 6](#_Toc49176273)

[4.3. General Methodology 7](#_Toc49176274)

[5. API Requirement 9](#_Toc49176275)

[5.1. REQSOA001. PIN Change 9](#_Toc49176276)

[5.1.1. Business Requirement 9](#_Toc49176277)

[5.1.2. Message Specification 9](#_Toc49176278)

[5.2. REQSOA002. PIN Set 11](#_Toc49176279)

[5.2.1. Business Requirement 11](#_Toc49176280)

[5.2.2. Message Specification 11](#_Toc49176281)

[5.3. REQSOA003. PIN Clear 13](#_Toc49176282)

[5.3.1. Business Requirement 13](#_Toc49176283)

[5.3.2. Message Specification 13](#_Toc49176284)

[6. Reports 15](#_Toc49176285)

1. History of changes

|  |  |  |  |
| --- | --- | --- | --- |
| version | date | Description | author |
| 0.1 | 11.08.2020 | Initial Version | Tu B. Nguyen |
| 1.0 | 03.09.2020 | Final Version | Tu B.Nguyen |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Copyright**

© OpenWay Asia Limited 2020. All rights reserved.

The Copyright of this complete document and every part it belongs to OpenWay Asia Limited. Proprietary material, brand or product names of other parties or trademarks remain with their respective owners. You may not, except with our express written permission, distribute or commercially exploit the content. Nor may you transmit it or store it in any other website or other form of electronic retrieval system. Any sample data used in examples below are completely fictitious unless otherwise noted.

**Disclaimer**

This document and the OpenWay Asia software it describes are furnished by OpenWay Asia Limited under a Software Licensing Agreement, Consultancy Agreement, Variation Request or Confidentiality Agreement, and may be used or copied only in accordance with the terms of such Agreement. Neither this document nor the OpenWay Asia software it describes may be used, sold, transferred, copied, translated, reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, in whole or in part, other than in accordance with the terms of such Agreement, or otherwise without prior written consent of OpenWay Asia Limited.

This document describes a generic product or service and should be read in conjunction with other documents relevant to the configuration of any specific system. The licensee of OpenWay software or user of OpenWay Asia services is responsible for ensuring that the product or service described herein meets its own requirements

**Confidentiality**

The information contained in this Document is the property of OpenWay Asia Ltd and contains CONFIDENTIAL information that is produced solely for the benefit of the receiving party named on the front page of this document. The recipient should keep this document and all its information confidential. On no account should this document, in whole or in part, be used, sold, transferred, copied, translated, reproduced or transmitted in any form or by any means, electronic or mechanical, or disclosed or disseminated to any third party, without the express written permission of OpenWay Asia Ltd.

1. Introduction

This document contains the Configuration Details which the WAY4 ePIN API will be configured with in order to meet the Business Requirements of Orient Commercial Bank. It covers the different sections of the WAY4 ePIN API needed to be done in them.

In case a Business Requirements cannot be solved by a system configuration then the same will have to be solved as an Enhancement to the System. Enhancements to the system configuration must be explicitly stated herewith, otherwise configurations described or referenced by this document are assumed to be standard. Enhancements shall not include optional configurations.

* 1. Notations

Notations used in this document are listed in the table below.

***Table 1. Notations***

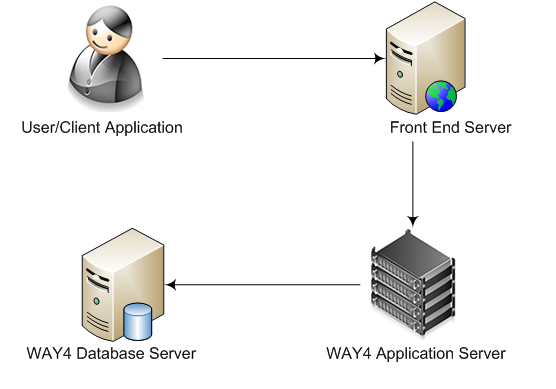
| Notation | Description |
| --- | --- |
| N | Numeric digits 0 through 9 |
| AN | Alphabetic and Special Characters |
| DT | Date + Format in field description |
| B | Binary representation of data |
| NVAR | Variable length data up to nn characters. There will be two or three character length (depending upon whether maximum data length is 99 or 999) at the beginning of the element to identify the number of positions following to the end of the data element |
| M | Mandatory |
| O | Optional |
| C | Conditional |
| NPA | NAPAS (National Payment Switch) |
| LC | Local Card |
| OCB | Orient Commercial Bank |
| OPW | OpenWay |

1. Introduction

## Overview

UFX services will be used as an interface between the WAY4 system and the outside system. For each UFX service, a UFX service request message is constructed by OpenWay and provided to external clients.

The diagram below indicates the global flow in the network:

Figure 1: WAY4 - UFX service Network

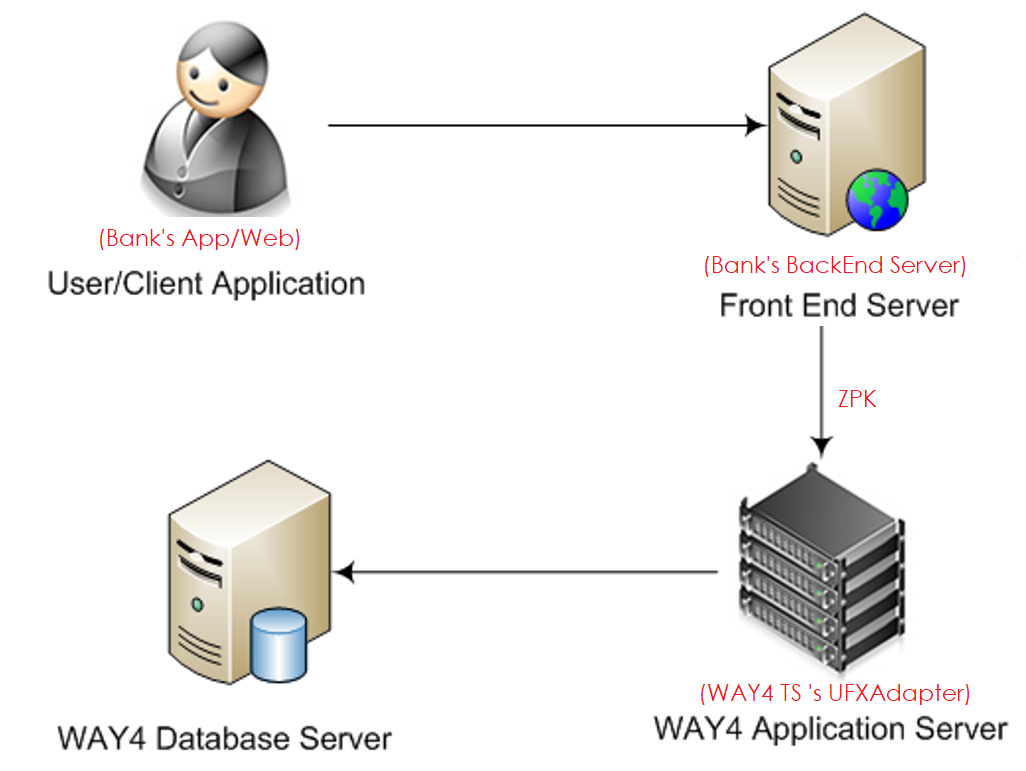
The flow is as follows:

* 1. A message/request is sent by the user/client application to OCB’s front-end server
  2. OCB’s front-end server is responsible to authenticate the request and perform all security checks to ensure that the message is valid and is originating from the expected source. Once the Security checks have passed, the call will be passed onto the WAY4 Application Server which will host the WAY4 UFX services.
  3. The WAY4 Application server verifies the request and transmits the request to the WAY4 database for data retrieval/processing.
  4. The WAY4 Database server process the request and return the requested information back to the WAY4 Application server to be routed to the user/client application.

**Implementation Steps at Bank**

In Bank, we consider the name of actor in figure 1 as follows:

* User/Client = Bank’s App/web
* Front End Server = Bank’s BackEnd Server
* Way4 Application server = Way4 Transaction Swicth



* Preparation Step:
  + Bank uses HSM to generate ZPK for WAY4 system (called WAY4 ZPK – encrypted format)
  + WAY4 ZPK is registered on WAY4Transaction Switch‘s UFX Adapter
  + Bank uses WAY4 ZPK as parameter to translate pin block from Bank’s session-ZPK to WAY4 ZPK.
  + Bank registers 1 POS contract in Way4 database to match with UFX message format. POS number is used source contract number in request message.
  + Protocol between Bank’s backend and Way4 Transaction Switch is http.
* Transaction Flow:
  + App/Web sends a request to Bank’s backend. Bank’s backend sends HSM command to generate Public key. Public key is responsed back App/web.
  + App/Web generates session-ZPK to encrypt clear PIN to PIN block. App/web use Public key to encrypt session-ZPK. PIN block and encrypted session-ZPK is sent to bank’s back end.
  + Bank’s back end sends the HSM command to translate PIN block under session-ZPK to WAY4 ZPK.
  + Bank’s back end call API to do Pin change/Pin set transaction, use Pin block under WAY4 ZPK as parameters.

## API List

Orient Commercial Bank(OCB) requests support for online XML services currently used to allow access to the WAY4 in-order to PIN set or PIN change for OCB’s card.

In WAY4 the XML online service implementation is called as UFX services and is referred to as the same in the rest of this document.

The following UFX services will be supported:

***Table 2. API function list***

|  |  |  |  |
| --- | --- | --- | --- |
| No | requirement | function | description |
| 1 | REQSOA001 | PIN Change | Allow cardholder to change from old PIN to new PIN |
| 2 | REQSOA002 | PIN Set | Allow cardholder to set him/her own PIN |
| 3 | REQSOA003 | Clear Old PIN | Allow cardholder clear old PIN before set new PIN |

## General Methodology

**Security Check**

OCB’s security requirements for UFX services will be managed by OCB and will not be in the scope for the current project. This includes any validation of the connection, authentication method and user or password validation.

**Request and Response Communication Method**

The UFX messages or services in WAY4 support the HTTP POST messages for receiving all incoming service requests. The WAY4 application server is the capable of processing these messages asynchronously i.e. it is possible for a requestor of a UFX service to send a second request without waiting for the response of the first request.

**Application Layer**

Every application layer message must have its own format. Currently, formats for representing the following service types have been implemented in the system:

* **Financial:** Allows retrieval of financial information like mini statement, statement (of various types), Additional services (example: PIN set and PIN change) and executing standing order requests. The Doc element specifies the structure of a message object.
* **Information:** Allows non-financial information on system objects such as "Contract" or "Client" to be required by their unique identifiers. The Information element specifies the structure of a message object. An object identifier is contained in the ObjectFor sub-element. Information about an object is contained in the DataRs sub-element of a response message.
* **Application:** Allows modification of non-financial objects such as "Contract" or "Client" and so on to be required. The Application element specifies the structure of a message object. Responses may contain either data received as a result of request processing or an indication of the request being accepted for processing. In the latter case, it is necessary to make an additional request to receive the required data. To specify a type of a request, the ResultDtls sub-element is used.

**Request Message ID**

When a message is send, a unique id for the message is created by the requestor, identifying the service request and it is recorded in the system of the requestor. This message ID is part of the header information for all UFX service requests which are received by WAY4. The requestor should put processes in place to ensure that the message ID generated is unique. This is because the same message ID will be sent as an echo field by WAY4 in the response message. The requestor can use this message ID to match the request to the response. It is recommended to generate value for this element basing on a "Universally Unique Identifier (UUID) URN Namespace", RFC 4122 specification.

**RRN**

RRN Stand for Retrieval Reference Number, which is unique database number of the original transaction corresponding to a document; when a sequence of documents is created e.g. in a dispute cycle or in case of a decline, WAY4 assigns the same RRN of the original transaction to each document in the sequence.

RRN must be generate base on Openway standard formula as below:

Formula: YDDDSSNNNNNN, where

* Y reflects the current year (last digit)
* DDD is the number of the day in the year (sometimes called the Julian date, although this is not quite correct)
* SS is the service identifier of the resource. In SOA this is the ID of WAY4GATE instance.
* NNNNNN is 6 digits of the cycle counter value.

**Institution ID – Access to Data**

Based on the Institution ID input parameter the service request must be validated to ensure that the service is requested for a card or merchant belonging to the same institution as the institution ID provided in the message.

The input parameters of all UFX services will be validated to ensure that they do not try to access entities which do not belong to their own institution.

Example A

WAY4: Card 1 in Institution A

UFX service: Update Card Status

UFX service Parameters: Institution B, Card 1

Result: Error, since Card 1 does not belong to Institution B

Example B

WAY4: Card 2 in Institution C

UFX service: Update Card Status

UFX service Parameters: Institution C, Card 2

1. API Requirement

## REQSOA001. PIN Change

### Business Requirement

From other system of OCB, message is sent to WAY4 to do PIN change transaction for cardholder.

### Message Specification

**Request Message**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field | DataType | M/O | Description | Notes |
| UFXMsg\MsgId | Char(24) | M | 24 characters |  |
| UFXMsg\Source app | Fix value | M | “IVR01” |  |
| UFXMsg\MsgData\Doc\TransType\TransCode\MsgCode | Fix value | M | “AddServReq” |  |
| UFXMsg\MsgData\Doc\TransType\TransCode\ServiceCode |  | M | **“CHANGE\_PIN”** |  |
| UFXMsg\MsgData\Doc\DocRefSet\Parm\ParmCode |  | M | RRN |  |
| UFXMsg\MsgData\Doc\DocRefSet\Parm\Value | Char(12) | M | Retrieve reference number |  |
| UFXMsg\MsgData\Doc\ Requestor\ContractNumber | Varchar(32) | M | Card contract number |  |
| UFXMsg\MsgData\Doc\ Requestor\ SecurityData\ SecParm\Code |  | M | **“PIN”** |  |
| UFXMsg\MsgData\Doc\ Requestor\ SecurityData\ SecParm\Type |  | M | **“01”** |  |
| UFXMsg\MsgData\Doc\ Requestor\ SecurityData\ SecParm\ HexData |  | M | **Old Pin block encrypted under ZPK followed the ISO 9564-1 format 0.** | **This shoud be done by front-end application.** |
| UFXMsg\MsgData\Doc\ Requestor\ SecurityData\ SecParm\Code |  | M | **“NEW\_PIN”** |  |
| UFXMsg\MsgData\Doc\ Requestor\ SecurityData\ SecParm\Type |  | M | **“01”** |  |
| UFXMsg\MsgData\Doc\ Requestor\ SecurityData\ SecParm\ HexData |  | M | **New Pin block encrypted under ZPK followed the ISO 9564-1 format 0.** | **This shoud be done by front-end application.** |
| UFXMsg\MsgData\Doc\ Source\ContractNumber | Varchar(32) | M | Device contract number |  |

Request sample



**Response Message**

|  |
| --- |
| <UFXMsg direction="Rs" msg\_type="Doc" scheme="WAY4USec" version="2.0" resp\_class="I" resp\_code="0" resp\_text="Success">  <MsgId>AAA-EEE-23124150</MsgId>  <Source app="IVR01" />  <MsgData>  <Doc>  <TransType>  <TransCode>  <MsgCode>AddServReq</MsgCode>  <ServiceCode>CHANGE\_PIN</ServiceCode>  </TransCode>  </TransType>  <DocRefSet>  <Parm>  <ParmCode>DRN</ParmCode>  <Value>28008016</Value>  </Parm>  <Parm>  <ParmCode>RRN</ParmCode>  <Value>200526190310</Value>  </Parm>  <Parm>  <ParmCode>AuthCode</ParmCode>  <Value>717102</Value>  </Parm>  </DocRefSet>  <Requestor>  <ContractNumber>9704380028930432</ContractNumber>  </Requestor>  <Source>  <ContractNumber>00100028</ContractNumber>  </Source>  <Status>  <RespClass>Information</RespClass>  <RespCode>0</RespCode>  <RespText>Success</RespText>  </Status>  </Doc>  </MsgData>  </UFXMsg |

## REQSOA002. PIN Set

### Business Requirement

From other system of OCB, message is sent to WAY4 to do PIN set transaction for cardholder.

Note: OCB system must call API “PIN clear” before calling “PIN Set” API.

### Message Specification

**Request Message**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field | DataType | M/O | Description | Notes |
| UFXMsg\MsgId | Char(24) | M | 24 characters |  |
| UFXMsg\Source app | Fix value | M | “Web01” |  |
| UFXMsg\MsgData\Doc\TransType\TransCode\MsgCode | Fix value | M | “AddServReq” |  |
| UFXMsg\MsgData\Doc\TransType\TransCode\ServiceCode |  | M | “CHANGE\_PIN” |  |
| UFXMsg\MsgData\Doc\TransType\TransRules\TransRule\ParmCode |  | M | “ProcessingMode” |  |
| UFXMsg\MsgData\Doc\TransType\TransRules\TransRule\Value |  | M | “Request” |  |
| UFXMsg\MsgData\Doc\TransType\TransRules\TransRule\ParmCode |  | M | “TrustedSource” |  |
| UFXMsg\MsgData\Doc\TransType\TransRules\TransRule\Value |  | M | “IVR” |  |
| UFXMsg\MsgData\Doc\LocalDt | Datetime | M | Transaction date |  |
| UFXMsg\MsgData\Doc\DocRefSet\Parm[ParmCode='RRN'].Value | Char(12) | M | Retrieve reference number |  |
| UFXMsg\MsgData\Doc\ Requestor\ContractNumber | Varchar(32) | M | Card contract number |  |
| UFXMsg\MsgData\Doc\ Requestor\CardInfo\CardExpiry | YYMM | M | Card Expired date |  |
| UFXMsg\MsgData\Doc\ Requestor\ SecurityData\ SecParm\Code |  | M | **“NEW\_PIN”** |  |
| UFXMsg\MsgData\Doc\ Requestor\ SecurityData\ SecParm\Type |  | M | **“01”** |  |
| UFXMsg\MsgData\Doc\ Requestor\ SecurityData\ SecParm\ HexData |  | M | **New Pin block encrypted under ZPK followed the ISO 9564-1 format 0.** | **This should be done by front-end application.** |
| UFXMsg\MsgData\Doc\ Source\ContractNumber | Varchar(32) | M | Device contract number |  |

Request sample



**Response Message**

|  |
| --- |
| <UFXMsg direction="Rs" msg\_type="Doc" resp\_class="I" resp\_code="0" scheme="WAY4Doc" version="2.0">  <MsgId>AAA-555-333-EEE-23124141</MsgId>  <Source app="IVR01"/>  <MsgData>  <Doc>  <TransType>  <TransCode>  <MsgCode>AddServReq</MsgCode>  <ServiceCode>CHANGE\_PIN</ServiceCode>  </TransCode>  </TransType>  <DocRefSet>  <Parm>  <ParmCode>RRN</ParmCode>  <Value>556599222222</Value>  </Parm>  <Parm>  <ParmCode>AuthCode</ParmCode>  <Value>111222</Value>  </Parm>  </DocRefSet>  <Description/>  <Requestor>  <ContractNumber>4015500174811772</ContractNumber>  <SecurityData>  <SecParm>  <Code>PIN\_RC</Code>  <Value>1</Value>  </SecParm>  </SecurityData>  </Requestor>  <Source>  <ContractNumber>99999997</ContractNumber>  </Source>  <DataRs/>  <Status>  <RespClass>Information</RespClass>  <RespCode>0</RespCode>  <RespText>Successfully completed</RespText>  </Status>  </Doc>  </MsgData>  </UFXMsg> |

## REQSOA003. PIN Clear

### Business Requirement

This section describes the SOA request for Erase old pin before doing the set pin operation.

### Message Specification

**Request Message**

|  |
| --- |
| <UFXMsg direction="Rq" msg\_type="Application" version="2.0">  <MsgId>AAA-555-333-EEE-23124141</MsgId>  <Source app="Web01"/>  <MsgData>  <Application>  <RegNumber>AA\_XML\_20\_9</RegNumber>  <OrderDprt>0101</OrderDprt>  <ObjectType>Card</ObjectType>  <ActionType>Update</ActionType>  <ObjectFor>  <ContractIDT>  <ContractNumber>1000050102847731</ContractNumber>  <Client>  <ClientInfo>  <ShortName><<<NONE>>></ShortName>  </ClientInfo>  </Client>  </ContractIDT>  </ObjectFor>  <Data>  <ProduceCard>  <CardExpiry>1306</CardExpiry>  <CommentText>Erase PIN</CommentText>  <AddData>  <Parm>  <ParmCode>ErasePIN</ParmCode>  <Value>Yes</Value>  </Parm>  </AddData>  </ProduceCard>  </Data>  </Application>  </MsgData>  </UFXMsg> |

**Response message**

|  |
| --- |
| <UFXMsg direction="Rs" msg\_type="Application" resp\_class="I" resp\_code="0" resp\_text="Successfully processed" version="2.0">  <MsgId>AAA-555-333-EEE-23124141</MsgId>  <Source app="Web01"/>  <MsgData>  <Application>  <RegNumber>AA\_XML\_20\_9</RegNumber>  <ObjectType>Card</ObjectType>  <ActionType>Update</ActionType>  <Status>  <RespClass>Information</RespClass>  <RespCode>0</RespCode>  <RespText>Successfully processed</RespText>  </Status>  </Application>  </MsgData>  </UFXMsg> |

1. Reports

No report is requested.