Discovery Report

Volume 9. MasterCard 3D Secure 2.0 - ACS

Orient Commercial Bank

Version 0.1

Status: Draft

Date: 27.10.2020

Prepared by: OpenWay

Author: Tu B. Nguyen

Approved By: Tu B. Nguyen

1. Table of Contents

[1. Table of Contents 2](#_Toc54771779)

[2. History of changes 3](#_Toc54771780)

[3. Introduction 4](#_Toc54771781)

[3.1. Notations 4](#_Toc54771782)

[4. System Overview 6](#_Toc54771783)

[4.1. WAY4 System Overview 6](#_Toc54771784)

[4.2. WAY4 3D Secure 1.0 – ACS Overview 6](#_Toc54771785)

[4.3. WAY4 3D Secure 2.0 – ACS Solution 7](#_Toc54771786)

[4.4. 3D Secure 2.0 Authentication Process Flows 7](#_Toc54771787)

[4.5. Project Scope 8](#_Toc54771788)

[5. Configuration Requirement 9](#_Toc54771789)

[5.1. REQC001. New 3D Secure 2.0 Protocols 9](#_Toc54771790)

[5.1.1. Business Requirement 9](#_Toc54771791)

[5.1.2. Technical Details 9](#_Toc54771792)

[5.2. REQC002. Authentication Methods 10](#_Toc54771793)

[5.2.1. Business Requirement 10](#_Toc54771794)

[5.2.2. Technical Details 10](#_Toc54771795)

[5.3. REQC003. Security Device 11](#_Toc54771796)

[5.3.1. Business Requirement 11](#_Toc54771797)

[5.3.2. Technical Details 11](#_Toc54771798)

[6. Integration Requirements 12](#_Toc54771799)

[6.1. REQI001. Directory Server - WAY4 ACS 12](#_Toc54771800)

[6.1.1. Business Requirement 12](#_Toc54771801)

[6.1.2. Technical Details 12](#_Toc54771802)

[6.1. REQI002. Client Application - WAY4 ACS 13](#_Toc54771803)

[6.1.1. Business Requirement 13](#_Toc54771804)

[6.1.2. Technical Details 13](#_Toc54771805)

[6.2. REQI003. Risk Based Authentication 14](#_Toc54771806)

[6.2.1. Business Requirement 14](#_Toc54771807)

[6.2.2. Technical Details 15](#_Toc54771808)

[6.3. REQI004. Other Requirement 16](#_Toc54771809)

[6.3.1. Business Requirement 16](#_Toc54771810)

[6.3.2. Technical Details 16](#_Toc54771811)

[7. Reconciliation 17](#_Toc54771812)

1. History of changes

|  |  |  |  |
| --- | --- | --- | --- |
| version | date | Description | author |
| 0.1 | 27.10.2020 | Initial 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 VCCS Acquiring will be configured with in order to meet the Business Requirements of Orient Commercial Bank. It covers the different sections of the WAY4 VCCS Acquiring 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

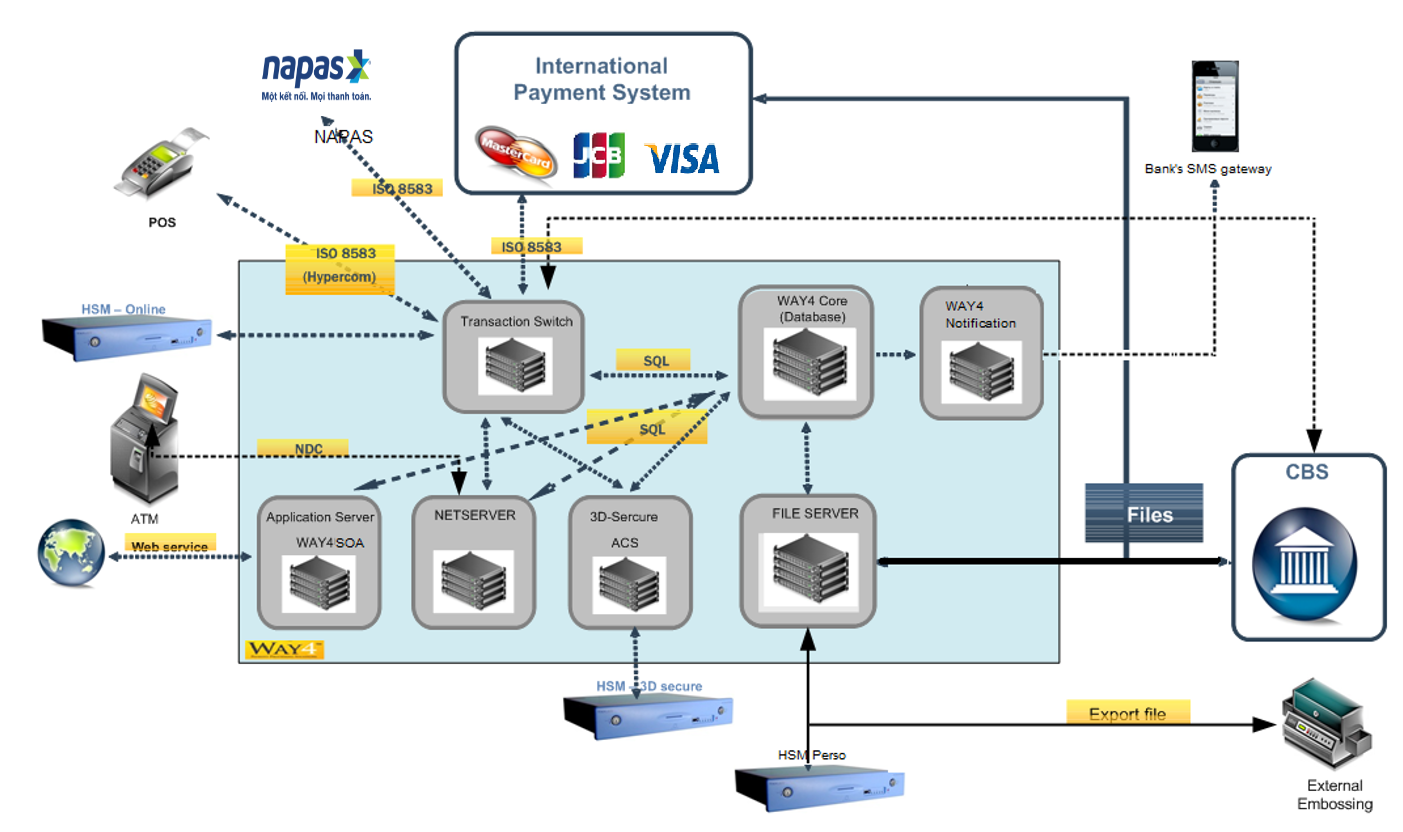
Notations used in this document are listed in the table below.

***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 |
| VCCS | Vietnam Chip Card Specificaiton |
| OCB | Orient Commercial Bank |
| OPW | OpenWay |
| CCD | Common Core Definitions |
| CDA | Combined DDA/Application Cryptogram Generation |
| CB | Certification Body |
| CDOL | Card Risk Management Data Object List |
| DDOL | Dynamic Data Authentication Data Object List |
| DOL | Data Object List |
| IAC | Issuer Action Code |
| IADOL | Issuer Application Data Object List |
| PDOL | Processing Options Data Object List |
| PIN | Personal Identification Number |
| UCOL | Upper Consecutive Offline Limit |
| UN | Unpredictable Number |
| RID | Registered Application Provider Identifier |
| PSN | PAN Sequence Number |
| PK | Public Key of a asymmetric key pair |
| CVM | Cardholder Verification Method |

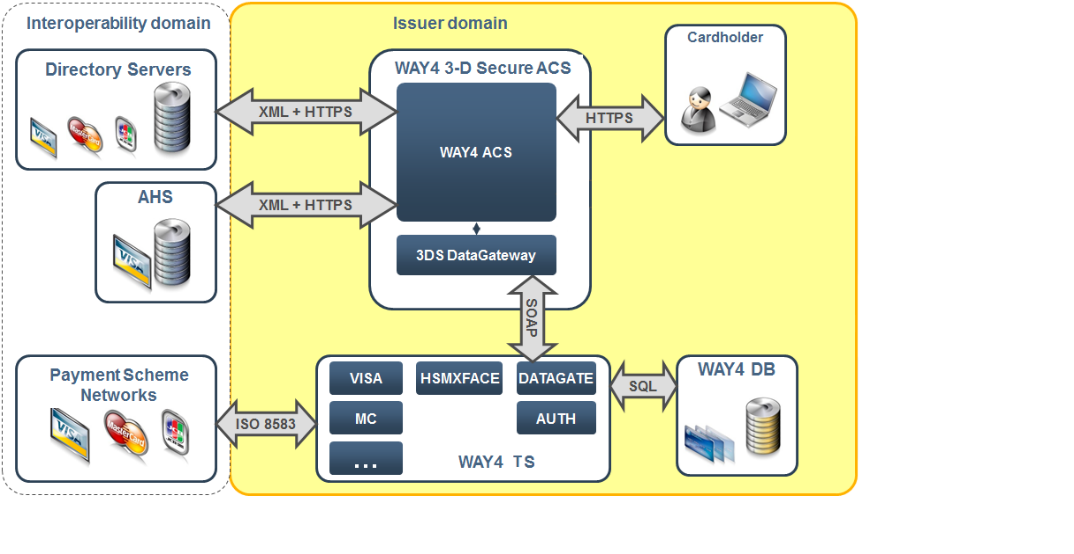
1. System Overview

## WAY4 System Overview

WAY4 system was implement on the year 2018. All cardholder and merchant data were migrated

In order to protect cardholder, OCB did implement 3D secure 1.0 – ACS from that time. Now, OCB want to upgrade version from 1.0 to 2.0 for 3D secure – ACS.

## WAY4 3D Secure 1.0 – ACS Overview

OCB had been implemented WAY4 3D Secure 1.0 – ACS. The diagram which is implemented as below:

The following list of functionalities will be launched in production:

* OCB 3D Secure - ACS supporting 3DS protocol version 1.0
* All MASTERCARD cards enrolled into Verified by MASTERCARD 3Ds 1.0 program.
* Configured authentication method - OTP send via SMS and Email.

## WAY4 3D Secure 2.0 – ACS Solution

The differences between current system diagram and proposed system diagram -no new modules will be installed, existing modules (3D ACS 1.0, 3D Secure Gateway, Auth Service) will be upgraded, integration with external biometrical service will be established.

Communications Directory Server - OCB ACS and OCB ACS - 3DS Client will happen with JSON messages where:

* AReq-ARes messages are pairs of authentication messages used to decide if transaction can go via frictionless flow (without client passing challenge like OPT via SMS), challenging flow (with client passing challenge like OPT via SMS) or if it should be declined.
* CReq-CRes messages are pairs of challenge messages used to pass selected authentication method in challenging flow. These messages are not send if ACS returns ARes saying that transaction successfully passed frictionless flow.
* RReq-RRes messages are pairs of results messages that confirm to acquirer through directory server that client successfully passed challenge.
* After implementing 3DS 2.0, Way4 ACS will support both version 3DS 1.0 and 2.0 exist in parallel on same ACS and public domain with different ports.

## 3D Secure 2.0 Authentication Process Flows

EMV 3DS supports two primary authentication flows:

* Frictionless Flow: Frictionless Flow occurs when Issuer authenticates the cardholder without cardholder involvement by evaluating the transaction’s risk level
  + The Merchant environment sends an authentication request message to the Issuer with all the required data to facilitate risk-based authentication
  + The Issuer receives the authentication request message and uses the data to evaluate the transaction’s risk. The Issuer returns an authentication response, and no additional cardholder verification required.
  + The merchant includes the MasterCard Authentication Data received from the authentication process in the authorization message
* Challenge Flow: A Challenge Flow occurs where the issuer interacts with the cardholder to complete authentication. The Challenge Flow occurs when the issuer assesses the risk of the transaction during the frictionless flow and determines that the transaction requires additional cardholder authentication, the frictionless flow transitions into the challenge flow:
  + The issuer communicates to the merchant environment that additional authentication is required to verify the identity of the cardholder
  + The merchant environment sends the issuer a challenge request message
  + The issuer authenticates the cardholder using their chosen challenge method such as a one-time passcode
  + Assuming authentication is successful, the transaction proceeds to authorization and the merchant includes key data elements from the authentication process in the authorization message.

If Merchant does not support 3D Secure 2.0, the ACS 3DS 1.0 flow will be used depend on message sent from merchant

## Project Scope

OpenWay will implement:

* EMV 3DS 2.0 for MasterCard
* Standard Risk Based Assessment Functionality
* Biometric Authentication via external authentication application/service
* One-time password via SMS and Email.

1. Configuration Requirement

## REQC001. New 3D Secure 2.0 Protocols

### Business Requirement

New protocol 3DS 2.0 is required for OCB to fulfill MASTERCARD requirements.

All MASTERCARD cards should be enrolled for 3DS 2.0 by default.

### Technical Details

WAY4 will support the setup and configuration. To use new protocol the following modules should be upgraded to the latest version:

* WAY4 ACS
* eGateway
* Application Server
* Transaction Switch
* CAVV Usage

## REQC002. Authentication Methods

### Business Requirement

Authentication methods available for MASTERCARD, cards should fulfill 3Ds ACS 2.0 requirements. The main requirements are:

* Frictionless Authentication through Risk Based Authentication (OpenWay RBA)
* Challenge Authentication with one of the following approved challenge methods:
  + Email with one-time use passcode
  + SMS with one-time use passcode
  + Biometric Authentication via external authentication application/service, able to support both mobile and web browser transaction.

WAY4 responsibility here is:

* Generation and verification of OTP entered by cardholder (for Email and SMS OTP authentication)
* Send OTP in text message to OCB SMSGateway.
* Biometric(OPW provided API allow to implement biometric)

New configuration shouldn't affect existing one for MASTERCARD cards.

### Technical Details

Risk based Authentication will be covered by Risk Based Assessment feature integrated to the standard WAY4 3DS ACS solution based on usage limiters as an add on functions of OpenWay Realtime Issuing Risk Monitoring.

Upgrade of Authentication Server to the latest is required.

One-time Passcode through SMS/Email will be implemented with reuse of the existing configuration.

Biometric authentication done by external authentication application integrated with WAY4.

Authentication Server is one of primary authentication method. The message exchanged between external authentication application and Way 4 Authentication Server is defined in the Way4 External Authentication API document.

Whether the transactions occur on website or merchant’s application, ACS receives the same information which is defined by EMVCo specifications.

Specification:

## REQC003. Security Device

### Business Requirement

OCB will use Safenet Protect Server External as HSM. HSM will be used to store certificates private keys as well as for OTP generation and check (This is security requirement of IPS).

Safenet is HSM for 3DSecure, Thales is online HSM to generate CAVV. When implementing, it may be changed and will be updated in testing certification. HSM online have to support LIC005.

### Technical Details

WAY4 3D Secure 2.0 - ACS will support this function as standard.

1. Integration Requirements

## REQI001. Directory Server - WAY4 ACS

### Business Requirement

Setup safe interfaces for message exchange between DS MASTERCARD and OCB ACS.

New setup shouldn't affect existing ACS 1.0 and other opponents of 3DS service of OCB.

### Technical Details

To setup interface between Directory Server and OCB ACS two certificates will be generated.

Server certificate ACS\_AREQ\_MA2/ ACS\_AREQ\_VA2 should be generated to:

Authenticate DS MASTERCARD at ACS side during AReq/ARes message exchange;

Encrypt data between ACS and DS MASTERCARD during AReq/ARes message exchange.

Client certificate ACS\_RREQ\_MA2/ ACS\_RREQ\_VA2 should be generated to authenticate OCB ACS at DS MASTERCARD side during RReq/RRes message exchange.

* 1. REQI002. Client Application - WAY4 ACS

### Business Requirement

Setup safe interfaces between application and ACS for challenging flow.

### Technical Details

To setup interface between Client's Application (APP) and OCB ACS certificate ACS\_SIGN\_MA2/ ACS\_SIGN\_VA2 should be generated to sign data in AReq/ARes messages that will be used for safe message exchange between APP and OCB ACS during challenge request.

* 1. REQI003. Risk Based Authentication

### Business Requirement

Remain all standards and functions described in Configuring WAY4™ e-Commerce Issuing Risk Based Assessment document of OpenWay.

14 RBA standard risk rules:

|  |  |  |  |
| --- | --- | --- | --- |
| No | rule | priority | result |
| 1 | LocalRiskMerchant – the rule checking the risked merchants in the certain area | 300 | Deny |
| 2 | CURRENCY\_RULE – the rule checking the exception lists related to the authentication currencies. | 310 | Deny |
| 3 | CountryMIDDeny – the rule to check the combination of suspicious IP country and suspicious MID | 320 | Deny |
| 4 | FREQUENZ – the rule checking the frequency of the purchases | 110 | Allow |
| 5 | NEGATIVECOUNTRY – the rule checking the suspicious IP country | 330 | Deny |
| 6 | NegativeCountryListDeny – the rule checking the list | 340 | Deny |
| 7 | NegativeDeviceID – the rule to check the list of suspicious device IDs | 350 | Deny |
| 8 | TRUSTEDIP – the rule to check the trusted list of Ips | 120 | Allow |
| 9 | Untrusted IP Check – the rule to check the authentication against the suspicious IP list | 360 | Deny |
| 10 | UserMFP DoNotMatch – the rule to check if the authentication’s fingerprint does not match previous values for the last 365 days | 200 | Force |
| 11 | UserMFP Match – the rule to check if the authentication’s fingerprint matches the history of fingerprints | 130 | Allow |
| 12 | ZERO\_AMOUNT – the rule to check the amount of the authentication | 140 | Allow |
| 13 | IPRISKEVALVELOCITY – the rule to check if there changes of the IP addresses for the user within the given time period | 210 | Force |
| 14 | ZONEHOPPING – the rule to check the user’s locations within the given time period | 220 | Force |

In addition, RBA can support following criteria:

* OCB can add, remove and modify RBA risk rules which can combine different conditions and also adjust the parameters of each rule
* Any transaction which does not hit any RBA risk rules need to be authenticated with challenge flow.
* RBA risk rules can be set in priority order, and the RBA system will process on this order: Number 1 is the lowest priority. Number 2 is the second lowest priority so on.
* Each rule will have unique priority.
* Have GroupList for OCB to group the parameter into 1 group to set the flow. The set of possible values for the lists is:
  + Currency – a list of three-digit currency codes.
  + Country – a list of two letters country codes.
  + IP – a list of IP addresses, "%" can be used for a mask (example – "192.168.%.%" to set the rule for all of IPs starting with 192.168).
  + Device ID – eight-digit device id.
  + MID – a list of merchant ID formatted in number and text
  + Merchant Name - a list of merchant names formatted in number and text
* The default currency for rule setting is converted to VND.
* Have On/Off button on usage limit to turn on/off for 1 specific card for each RBA rule.
* Have Active/Inactive button for each rule so that OCB may active/inactive 1 specific rule in each period for specific card number

### Technical Details

Way4 RBA module allows users to use both standard payment system parameters and their own customised parameters to configure risk rules.

Risk rules specified by usage limiters can have threshold values for the amount and/or number of transactions; if a transaction exceeds the threshold value, it is considered suspicious. These limiters are analysed during 3-D Secure authentication.

* 1. REQI004. Other Requirement

### Business Requirement

* Ensures the connection with MasterCard system and other internal system
* Able to receive and process all new data from merchant in 3DS 2.0
* OCB can add, adjust, remove RBA rules or parameters internally
* After implementing 3DS 2.0, Way4 ACS can support both version 3DS 1.0 and 2.0 exist in parallel on same ACS and public domain with different ports
* OpenWay will transfer all source codes to build reports and instruction for OCB to build and customize reports internally.

### Technical Details

We will implement thest in WAY4.

1. Reconciliation

No Apply for Authentication message.