⌂ > ... > MyDebit > Overview > MyDebit Cnp For Acquirer

MyDebit Secure Implementation for Acquirer

Introduction

Acquirer is a business entity (can be a financial or non-financial institution) that establishes a contractual service relationship with a Merchant for the purpose of accepting payment Cards. In the context of 3DS, in addition to the traditional role of receiving and sending Authorisation and settlement messages (enters transaction into interchange), the Acquirer also determines whether a Merchant is eligible to support and participate in 3DS.

MyDebit Secure Program for Acquirer

The key system components of the Acquirer Domain are 3DS Server. Together with 3DS Client, this client-server system is referred to as 3DS Requestor, aka the Merchant system. 3DS Client provides the front-end interface to the consumer and passes the information of the purchase to the 3DS Server. 3DS Server initiates the authentication request to the DS which in turn forward the request to the respective Issuer.

Benefits to Acquirers

- Increased growth opportunities by providing better checkout experience to Cardholders
- Reduced liability for fraudulent activities
- Raised Merchants' brand reputation by taking an active role on transaction security

Acquirer Domain

The Acquirer Domain consists of the following components:

- 3DS Requestor Environment

- 3DS Requestor
- 3DS Server
    - Hosted Service
    - On-premises solution in Merchant’s system environment
- 3DS Client
    - Website/Browser
    - App (mobile device)
- Acquirer Host System (payment authorization)

Though 3DS Client is a component that resides on Cardholder’s device, it’s often an application that’s distributed by the Acquirer or Merchant.

Device Channels

Authentication is initiated by the 3DS Requestor Environment. The following type of device channels are supported:

- **App-based** - In this scenario, a Cardholder conducts a purchase transaction via a Merchant provided application on a mobile device such as a smartphone or a tablet. This application will have a 3DS-SDK embedded within to support the EMV 3DS protocol specification

- **Browser-based** - In this scenario, the device would have a default browser application. The device could be a mobile phone, tablet, or a regular laptop PC

- **3DS-Requestor-Initiated (3RI)** - In this case, the Cardholder may not be interacting with the Merchant when the 3DS request has been initiated. Instead the 3DS Request is initiated by the Merchant on behalf of the Cardholder base on the information previously provided by the Cardholder. No authorization process will take place. Merchants typically use such authentication method to verify that a subscribing customer has provided a valid form of payment. This method may also be used on a Telephone Order scenario.

MyDebit Secure Specific Static Settings for Acquirer

Data Element / Field Name	Source	Message	Description

3DS Server Reference Number
3DSServerRefNumber
	EMVCo	AREQ = R
		PREQ = R
			Unique identifier assigned by the EMVCo secretariat upon testing and approval

3DS Server Operator ID
threeDSServerOperatorID
	PayNet	AREQ = C
		PREQ = C
			PayNet-assigned unique 3DS Server identifier

3DS Server URL threeDSServerURL	Acquirer Domain	AREQ = R	Fully qualified URL of the 3DS Server to which the DS will send the RReq message after the challenge has completed
DS URL dsURL	PayNet	AREQ = C	URL of the DS to which the ACS will send the RReq if a challenge occurs. Required between the DS and ACS but will not be present from 3DS Server to DS
Cache Expiration Period	Acquirer Domain	-	The expiration period of the cache of card range information obtained via PREQ/PRES messages. Should be between 1 to 24 hours.
AREQ/ARES Message Timeout Period	Acquirer Domain	-	The timeout period from the sending of AREQ to the receiving of ARES. Should be more than 8 second since

Data Element / Field Name	Source	Message	Description
			the timeout period between DS and ACS is usually set at 8 second
PREQ/PRES Message Timeout Period	Acquirer Domain	-	The timeout period from the sending of PREQ to the receiving of PRES. Should be 2 second or more
Error Message Timeout Period	Acquirer Domain	-	Timeout period from the sending an Error message to the receiving of a response. Should be 2 second or more
Protocol Version Number	Acquirer Domain	-	The version number of EMV 3DS protocol active on this 3DS Server

3DS Server Implementation Steps

This section highlights for a Merchant or an Acquirer, the major milestones of a MyDebit Secure implementation projects. Time taken to execute for each task may vary for every implementation, hence the value stated in the project task list is only for reference.

No	Project Task	Involvement	Duration
1	Requirement gathering • Card Range Routing Strategy • Configurable at Merchant Account to opt-in and opt-out for MyDebit Secure	Acquirer 3DSS provider	3 weeks

No	Project Task	Involvement	Duration
	• Look and feel, design and prototyping • 3D Authentication data to be submitted to Acquiring Host • ISO and Settlement/Batch Upload Deployment for MyDebit Secure transaction		
2	Payment Gateway and 3DSS Application Development & Customization • Merchant Account Module Enhancement • Card Range Management • ISO and Settlement/Batch Upload Development 3DS2.0 Data Element and API Enhancement	3DSS provider	*6 weeks
3	Host Customization • Acquirer Host development to support MyDebit Secure	Acquirer	*6 weeks
4	Development/Test Environment Setup & Testing • Development testing • Test environment setup • SIT & UAT • Pre-live testing	Acquirer 3DSS provider	**3 weeks (subject to Issuer testing progress)

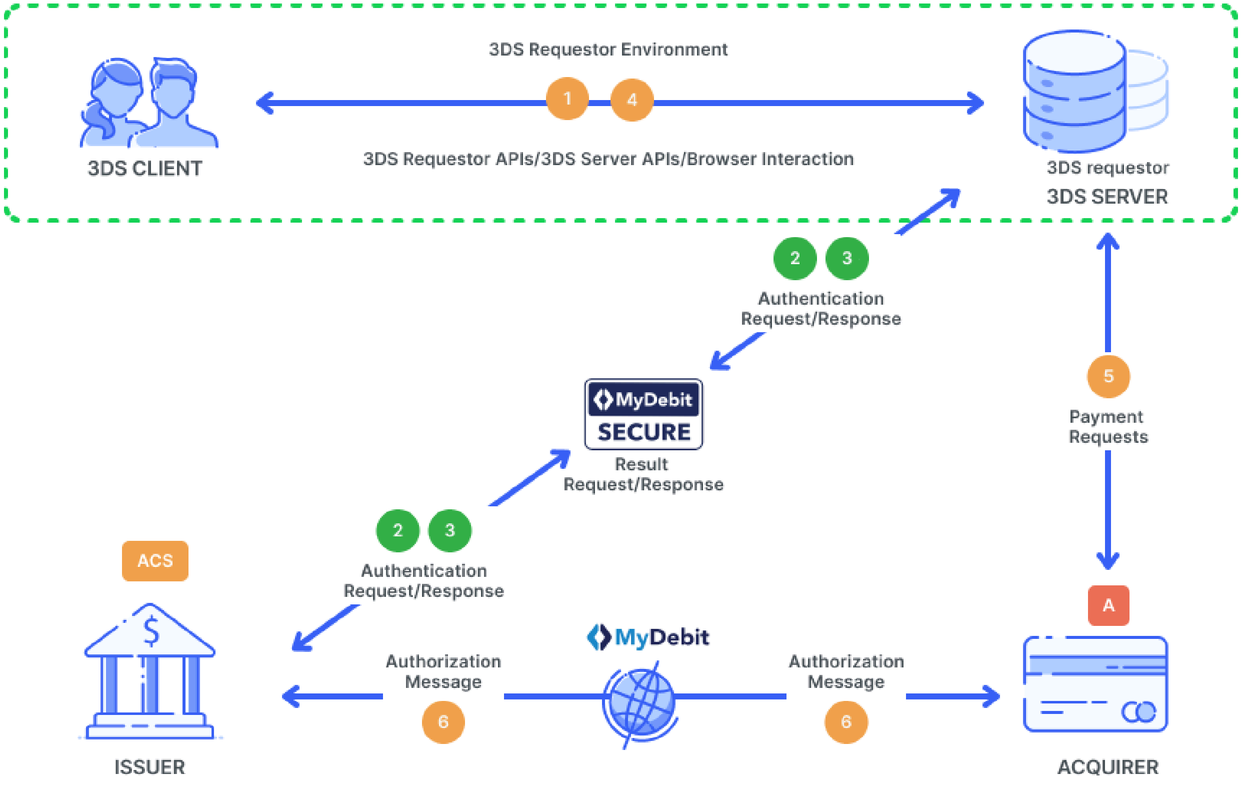
No	Project Task	Involvement	Duration
5	Certification and PIT • PayNet ISO8583 Certification if the Acquiring Host is not certified to support MyDebit Secure • PIT (Production Integration Test) with PayNet sandbox	Acquirer	**3 weeks (subject to Acquirer certification progress)
6	Production Environment Setup & Installation • Hardware/software, infrastructure configuration • Card Range Query (PReq and PRes) • Merchant Integration to Payment Gateway New API if new to support 3DS2.0	Acquirer 3DSS provider	3 weeks (subject to The Client readiness)
7	Training	Acquirer 3DSS provider	2 days

Note: *can happen concurrently **can happen concurrently

Authentication Routing

In order to initiate an Authentication Request with the correct DS, the 3DS Server is required to query the PayNet DS periodically to obtain the updated list of MyDebit BINs participating in the Program. The current recommendation is once every 24 hours.

The figure below is the illustration of the frictionless flow.



Steps	Description
1	**3DS Requestor Environment** — Within the 3DS Requestor Environment, the necessary 3-D Secure information is gathered and provided to the 3DS Server for inclusion in the AReq message.
2	**3DS Server through DS to ACS** — Using the information provided by the Cardholder and data gathered within the 3DS Requestor Environment, the 3DS Server creates and sends an AReq message to the DS, which then forwards the message to the appropriate ACS.

Steps	Description
3	**ACS through DS to 3DS Server** — In response to the AReq message, the ACS returns an ARes message to the DS, which then forwards the message to the initiating 3DS Server. Before returning the response, the ACS evaluates the data provided in the AReq message. In a Frictionless Flow, the ACS determines that further Cardholder interaction is not required to complete the Authentication.
4	**3DS Requestor Environment** — The 3DS Server communicates the result of the ARes message to the 3DS Requestor Environment which then informs the Cardholder.
5	**Merchant and Acquirer** — The Merchant proceeds with Authorisation exchange with its Acquirer. If appropriate, the Merchant, Acquirer or Payment Processor can submit a standard Authorisation request.
6	**Payment Authorisation** — The Acquirer can process an Authorisation with the Issuer through the Payment System and return the Authorisation results to the Merchant.

Authorization Routing

Upon the completion of the E3DS authentication process, the Acquirer needs to send the transaction via the MyDebit switch using ISO8583 message format to the Issuer for Authorization. In order to avoid mis-routing, Acquirer must adopt the methods listed below:

DS Transaction ID contains a pre-fix of “PN”

Recognize the new ECI values:

i. 15 – Fully Authenticated

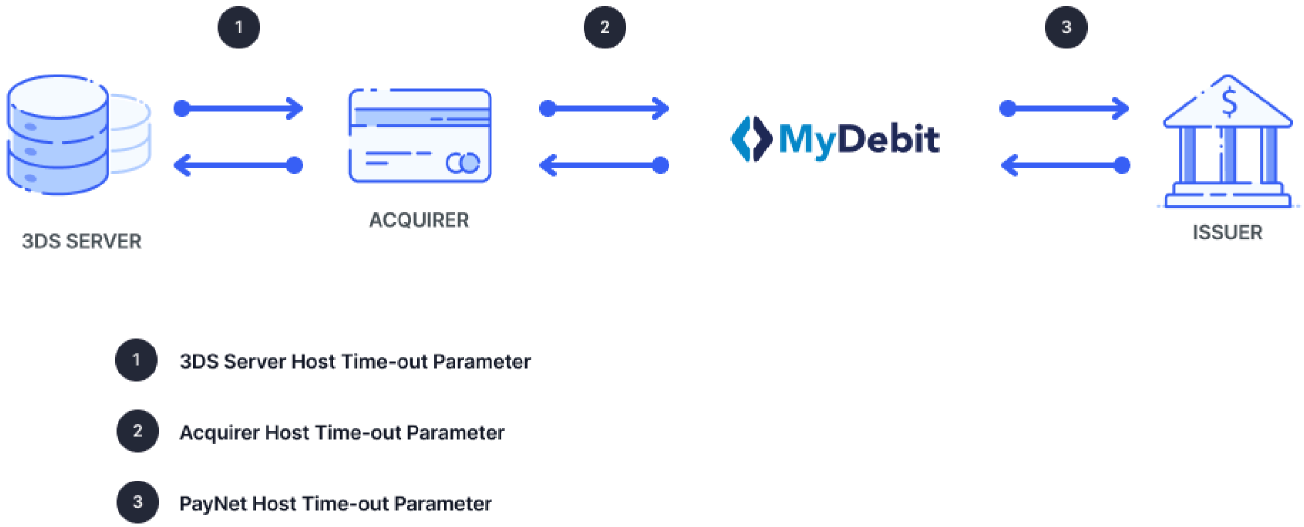
ii. 16 – Attempts Only

iii. 17 – Non-Authenticated

Synchronization of BIN table between acquiring host systems and 3DS Servers

Time Out Parameter Setting

Diagram below illustrates all types of MyDebit Card-Not-Present transaction’s time-out parameters namely as 3DS Server, Acquirer host and PayNet.


1
2
3
3DS SERVER
ACQUIRER
MyDebit
ISSUER
1 3DS Server Host Time-out Parameter
2 Acquirer Host Time-out Parameter
3 PayNet Host Time-out Parameter

3DS Server Host Time-out Parameter

As for MyDebit Secure (CNP), 3DS Server must set the time out parameter minimum 45 seconds.

Acquirer Host Time-out Parameter

This is an allowable period for the Acquirer host to wait a response message from MyDebit Switch before Acquirer host declines the transaction as a time-out. A time-out response message will be sent to 3SD Server. Acquirer host must be configured with the Acquirer Host Time-Out Parameter to 40 seconds.

MyDebit Switch Time-out Parameter

This is an allowable period for MyDebit Switch to wait a response message from Issuer host before MyDebit Switch declines the transaction as a time-out. A time-out response message will be sent to 3DS Server through Acquirer host. MyDebit Switch sets the time-out parameter to 30 seconds.