⌂ > ... > MyDebit > Overview > MyDebit Cnp For Issuer

MyDebit Secure Implementation for Issuer

Introduction

Issuer is a financial institution license to issue Cards, contracts with Cardholders to provide card services, determines eligibility of Cardholders and identifies Card number/BIN ranges to participate in the 3DS Program.

Benefits to Issuers

- Reduced risk of fraudulent activities - Increased growth opportunities
- Relatively easier implementation of a global EMV 3DS standard for authentication and keeping up with its development for future enhancements

> ⓘ **INFO**
>
> EMV is a term referring to EMVCo's specifications for global interoperability and acceptance of secure payment transactions and/or products and services complying with such specifications.

MyDebit Secure Program for Issuer

Access Control Server (ACS)

Access Control Server, ACS, is the key component of the Issuer Domain under the EMV 3DS specification. Its main function is to authenticate, frictionless or challenge, the consumer during a card-not-present transaction.

Issuer Domain

The Issuer Domain consists of the following components:

- Cardholder
- Consumer Device
- Issuer Host System
- Issuer Access Control Server

Serving the MyDebit Secure 3DS pages

In a transaction that requires challenging the Cardholder, the ACS provides the challenge UI for the Cardholder to enter the authentication information. Depending on the device in use, one of the three types of Challenge UI may be presented:

- Browser-based
- App-based (HTML)
- App-based (Native)

MyDebit Secure Specific Static Settings for Issuer

Data Element / Field Name	Source	Message	Description
ACS Reference Number acsReferenceNumber	EMVCo	ARES = R	Unique identifier assigned by the EMVCo Secretariat upon Testing and Approval
ACS Operator ID acsOperatorID	PayNet	ARES = C	PayNet-assigned unique ACS identifier

Data Element / Field Name	Source	Message	Description
ACS URL acsURL	Issuer Domain	Browser ARES = C	Fully qualified URL of the ACS to be used for the challenge
ACS Signed Content acsSignedContent	Issuer Domain	App ARES = C	Contains the JWS object (represented as a string) created by the ACS for the ARes message
Error Message Timeout Period	Issuer Domain	-	Timeout period from the sending an Error message to the receiving of a response
Protocol Version Number	Issuer Domain	-	The highest version supported. Must be backward compatible

Implementation Steps

This section highlights for an Issuer the major milestones of a MyDebit Secure implementation projects. Time taken to execute for each task may vary for every implementation, hence the durations stated in the project tasks list are only for reference.

No	Project Task	Involvement	Duration
1	Requirement gathering: • Card profile migration strategies • Mode of authentication & authentication process flow • Look and feel, design, prototyping • Secret Key for AV, migration strategies	Issuer ACS provider	3 weeks

No	Project Task	Involvement	Duration
	• OTP delivery channels • Authenticator Mobile Apps, if applicable • RBA profiling		
2	ACS Application Development & Customization • Database setup • Authentication module setup • Cardholder management system setup • Configuration for Authentication Secret Key (for PIAV) and its migration plan • OTP delivery channel(s) development	ACS provider	*6 weeks
3	Host Customization • Bank Host development if the host not ready to support EMV 3DS at the moment	Issuer	*6 weeks
4	Development/Test Environment Setup & Testing • Development testing • Test environment setup • SIT & UAT • Pre-live testing	Issuer ACS provider	**3 weeks (subject to Issuer testing progress)

No	Project Task	Involvement	Duration
5	Certification and PIT • PayNet ISO8583 Certification if the Issuing Bank Host is not certified to support EMV 3DS at the moment • PIT (Production Integration Test) with PayNet sandbox	Issuer	**3 weeks (subject to Issuer certification progress)
6	Production Environment Setup & Installation • Hardware/software, infrastructure configuration • Card profile enrolment to ACS • RBA profile setting, if applicable • Authentication mobile apps upload • Authentication Secret Key (for PIAV) installation or key migration	Issuer ACS provider	3 weeks (subject to The Client readiness)
7	Training	Issuer ACS provider	2 days

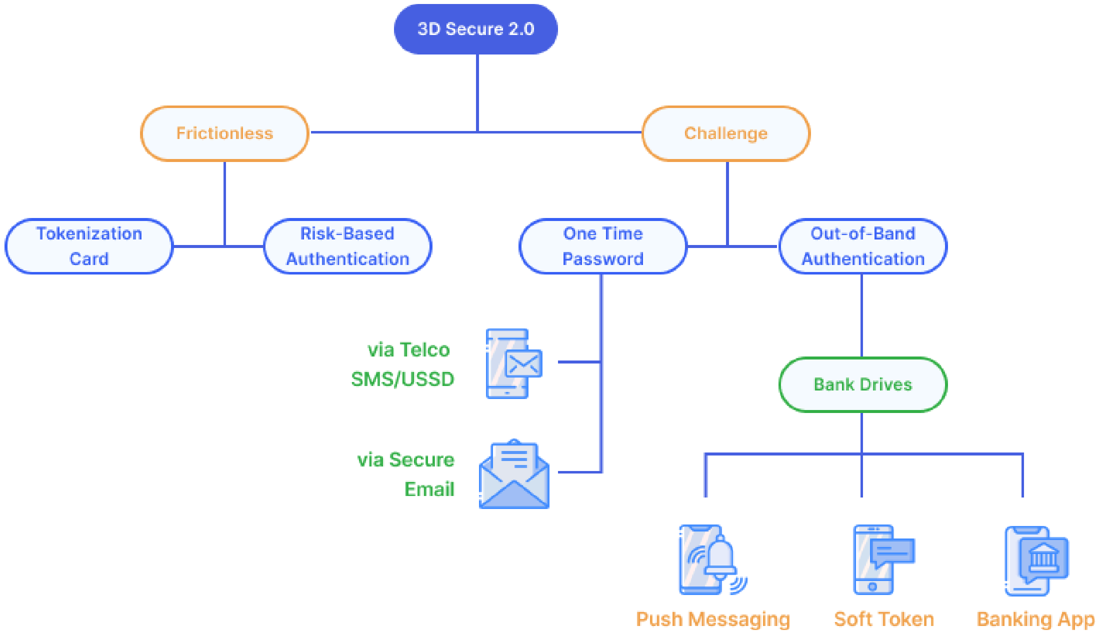
Note: *can happen concurrently **can happen concurrently

Frictionless flow vs Challenge flow

When receiving an AReq from DS, Issuers may apply different Authentication flows for different transaction environments. If the Issuer uses rules or data-analytic approach to assess the riskiness of a transaction, the Cardholder may experience a frictionless flow if the transaction is deemed low risk. Such Authentication method is known as Risk-Based Authentication.

For transactions that are required to go through the Challenge Flow, Issuer may also apply different authentication methods depending on the device channels in use, and the functional capabilities of the ACS.

The figure below is Various Authentication Flows and Methods.



Authentication Methods for Challenge Flow

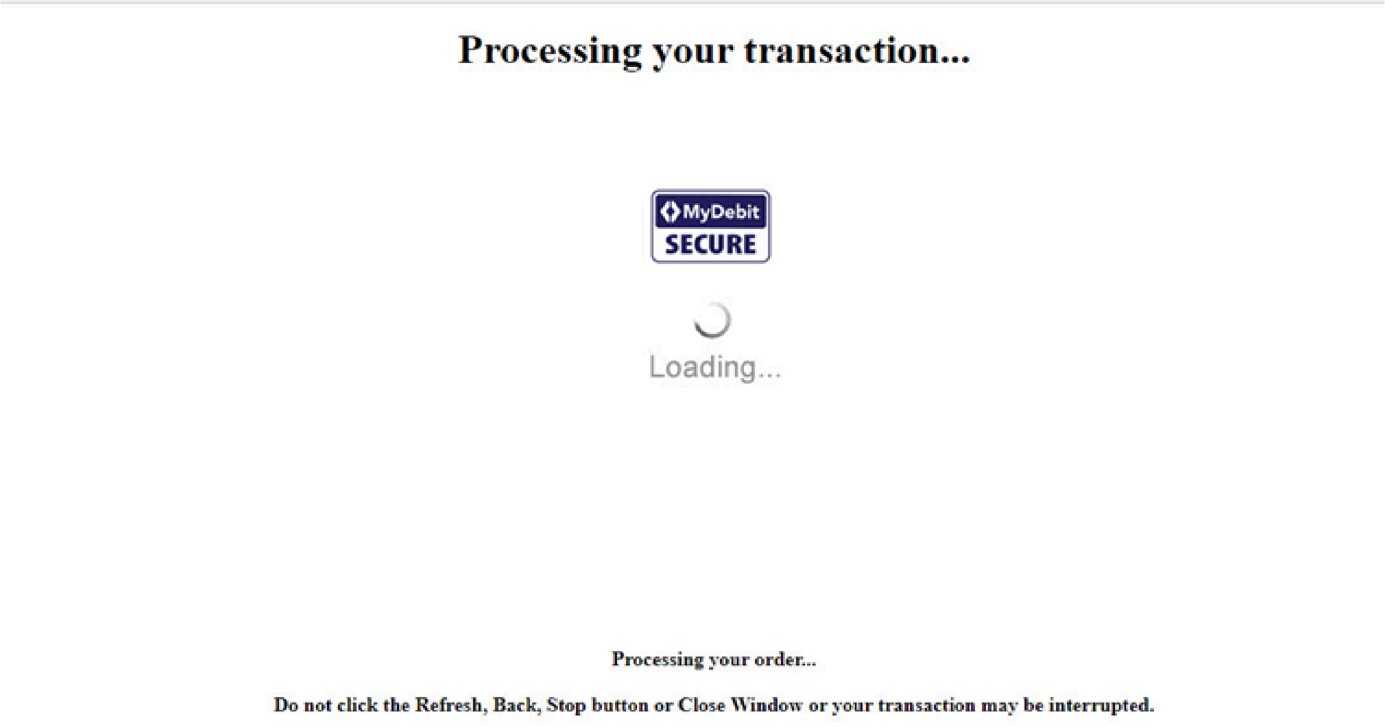
MyDebit Secure program does not support Static authentication type and methods. The table below is Authentication Types and Authentication Methods.

No	Authentication Type ARES/RREQ	Authentication Method RREQ
1	02 = Dynamic	02 = SMS OTP 03 = Key fob or EMV card reader OTP 04 = App OTP 05 = OTP Other 10 = Other
2	03 = OOB	07 = OOB Biometrics 08 = OOB Logins 09 = OOB Others

MyDebit Secure Branding Guide

MyDebit Secure is the Program name that consumers associate with during the authentication process. The figure below would be the initial screen right after the Cardholder click on the “Submit” button. If the transaction is to go Frictionless, this would be the only screen related to 3DS, and upon successful authorization from the Issuer, a “Confirmation” page from the Merchant would be presented to the Cardholder indicating the completion of the transaction.

Figure below Sample Processing Screen (Browser Lightbox).



Processing your transaction...

Loading...

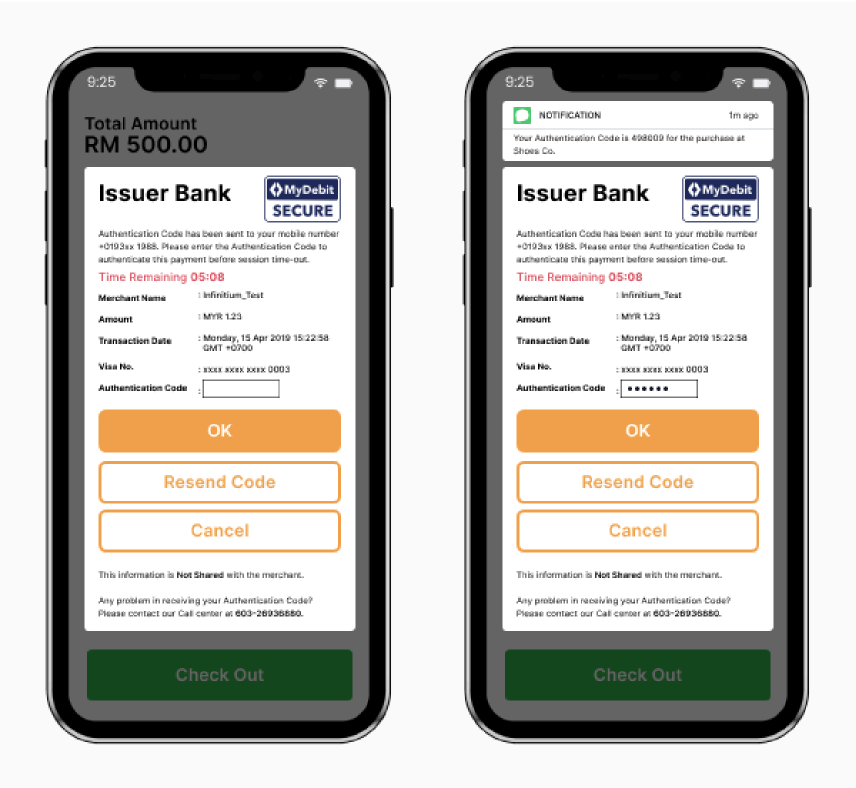
Processing your order...

Do not click the Refresh, Back, Stop button or Close Window or your transaction may be interrupted.

In a transaction that requires challenging the Cardholder, the ACS provides the challenge UI for the Cardholder to enter the authentication information. Depending on the device in use, one of the three types of Challenge UI may be presented:

- Browser-based
- App-based (HTML)
- App-based (Native)

The figure below is Sample Challenge UI Examples.



Authentication Code has been sent to your mobile number +0193xx 1988. Please enter the Authentication Code to authenticate this payment before session time-out.

Time Remaining 05:08

Merchant Name	: Infinitium_Test
Amount	: MYR 1.23
Transaction Date	: Monday, 15 Apr 2019 15:22:58 GMT +0700
Visa No.	: xxxx xxxx xxxx 0003
Authentication Code	:

This information is **Not Shared** with the merchant.

Any problem in receiving your Authentication Code? Please contact our Call center at **603-26936880.**

Your Authentication Code is 498009 for the purchase at Shoes Co.

Authentication Code has been sent to your mobile number +0193xx 1988. Please enter the Authentication Code to authenticate this payment before session time-out.

Time Remaining 05:08

Merchant Name	: Infinitium_Test
Amount	: MYR 1.23
Transaction Date	: Monday, 15 Apr 2019 15:22:58 GMT +0700
Visa No.	: xxxx xxxx xxxx 0003
Authentication Code	: ••••••

This information is **Not Shared** with the merchant.

Any problem in receiving your Authentication Code? Please contact our Call center at **603-26936880.**

ACS Functional Requirements

This section makes reference to the EMV 3-D Secure Protocol and Core Functions Specification. It explains the functional requirements of the ACS, the main system components of the Issuer Domain. The ACS may be operated by an Issuer or a service provider on-behalf-of the Issuer.

MyDebit Secure Certificates for ACS

All digital certificates will be generated/signed under the Program root cert. These certificates for an ACS include:

- TLS client and server certificates used in the establishment of the communication channels between the DS and the ACS

- Signing certificates used to sign messages by generating a digital signature, and the digital signature is passed from the ACS to the 3DS Server or 3DS SDK

The table below is Certificates involved in an EMV 3DS environment for Issuer.

Certificate Name	**Certificate Authority**	**Usage**
MyDebit Secure CA root certificate	Paynet	Validation of all certificates issued under the same PayNet program root
ACS server certificate	Paynet	TLS channel encryption between DS and ACS for AREQ/ARES
ACS client certificate	Paynet	TLS channel encryption between ACS and DS for RREQ/RRES
Commercial CA root certificate	Commercial CA	Validation of all certificates issued under the same CA root
Commercial server certificate (for cardholder device connection)	Commercial CA	TLS channel encryption between 3DS-SDK and ACS for CREQ/CRES
Commercial server certificate (for 3DS Method)	Commercial CA	TLS channel encryption between browser and ACS for 3DS Method