⌂ > ... > MyDebit > Overview > MyDebit Secure Card Not Present

MyDebit Secure Card-Not-Present (CNP)

Introduction

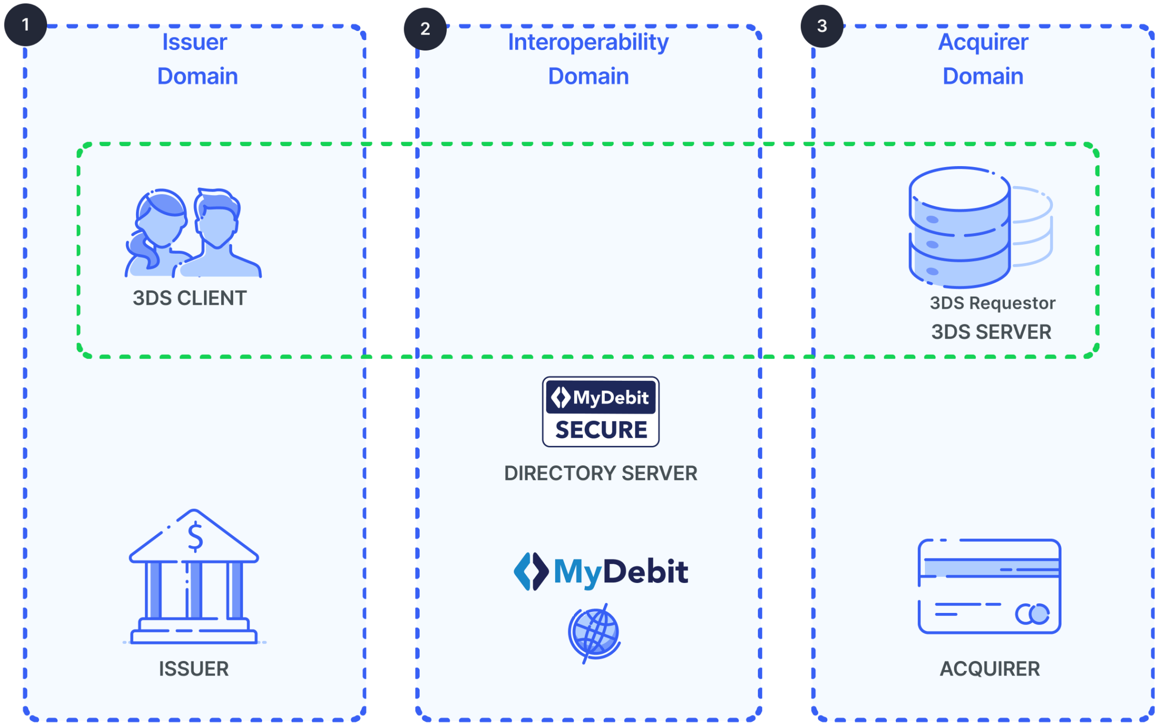
A Card-Not-Present (CNP) transaction is a retail spend transaction where the Cardholder is not physically present at the Merchant. While face-to-face, card-present, transactions are being secured with the deployment of EMV chip cards and chip card-reading terminals, fraudsters have shifted their attentions to Card-Not-Present (“CNP”) environment. The acceleration of smartphone penetration has also intensified the competitions among the various payment methods and networks. In order for MyDebit volume to grow in the e-commerce environment and to be accepted securely, PayNet is introducing MyDebit Secure. MyDebit Secure is a CNP authentication program (Program) whose protocol specification is developed based on EMV 3-D Secure (E3DS) Protocol and Core Functions Specification. 3-D Secure (3DS) is a protocol standard that is based on three-domain model where:

1. **The issuer domain** - comprise of cardholders, issuing FIs, who are connected to the system; and

2. **The interoperability domain** - operated by PayNet as the card network.

3. **The acquirer domain** - comprise of Merchants, payment gateways and acquiring Financial Institutions (“FIs”);

The figure below is Three-Domain MyDebit Secure.



ⓘ **INFO**

Check out the **glossary** which provides definitions and explanations of frequently used terms for MyDebit scheme. You may also refer to Abbreviations which been used in this document.

E3DS, which is owned and managed by EMVCo is the next generation of the industry standard for online authentication for e Commerce card payments. In comparison to the current 3DS, the E3DS has enhanced features as follows:

- Supports in-application purchases on mobile phone and other customer devices;
- Enables Issuers to perform risk-based decisions for frictionless cardholder authentication where customers may not be required to perform additional authentication; and

- Enables non-payment customer authentication for Identification & Verification (ID&V) services for mobile wallets and secure token requests for card on file.

> ⓘ **INFO**
>
> E3DS is an e-commerce authentication protocol that enables the secure processing of payment, non-payment and account confirmation card transactions that is governed by EMVCo.

Type of MyDebit Card-Not-Present Transactions

- **Online Transaction** - The Cardholder and the Card are usually in the same location and the merchant operates elsewhere. There is no face-to-face interaction with the Cardholder and the Merchant needs to take steps to check that they are dealing with genuine customer, carry out identity checking or perform 3D Secure. Online transaction is a real-time payment transaction initiated by the Cardholder, who is the retail customer, at the Merchant website or e-commerce application. The transaction is then routed via MyDebit Secure to the Issuer ACS for authorisation.

- **Card-On-File** - This occurs where a customer has provided a continuous authorisation on a debit or credit card to the Merchant, frequently for goods that are paid for on a subscription basis but where the value of the goods may vary (tokenisation of the card PAN to a token number for storage at the Merchant is required).

- **Recurring Billing** - Recurring payments are when a consumer agrees to pay for a product or service at specific intervals over a period of time, e.g., health club membership payments, insurance premiums, utility bills, subscription fees etc. The recurrence may be fixed with pre-determined renewal periods e.g., magazine subscription or continuing e.g., telephone bills and can occur monthly, quarterly, or annually.

Abbreviation	Descriptions
3DS	Three Domain Secure
3DS SDK	Three Domain Secure Software Development Kit
3RI	3DS Requestor Initiated
ACS	Access Control Server
AReq	Authentication Request
ARes	Authentication Response
AV	Authentication Value
AVS	Address Verification Service
BIN	Bank Identification Number
CA	Certificate Authority
CA DS	Certificate Authority Directory Server
CNP	Card-Not-Present
CReq	Challenge Request
CRes	Challenge Response
DS	Directory Server

Abbreviation	Descriptions
EC	Elliptic Curve
ECI	Electronic Commerce Indicator
JSON	JavaScript Object Notation
MAC	Message Authentication Code
NPA	Non-Payment Authentication
NVP	Name/value pair
OOB	Out-of-Band
PA	Payment Authentication
PAV	PayNet Authentication Value
PIAV	PayNet Issuer Authentication Value
OTP	One-time Passcode
PReq	Preparation Request Message
PRes	Preparation Response Message
RID	Registered Application Provider Identifier
RReq	Results Request Message

Abbreviation	Descriptions
RRes	Results Response Message
RSA	Rivest–Shamir–Adleman
SDK	Software Development Kit
TLS	Transport Layer Security
URL	Uniform Resource Locator
UUID	Universally Unique Identifier

Definition

The following terms are used in the document.

Abbreviation	Descriptions
3DS Client	The consumer-facing component allowing consumer interaction with the 3DS Requestor for initiation of the EMV 3-D Secure protocol.
3DS Integrator	An EMV 3-D Secure Participant that facilitates and integrates the 3DS Requestor Environment, and optionally facilitates integration between the Merchant and the Acquirer.
3DS Method	A scripting call provided by the 3DS Integrator that is placed on the 3DS Requestor website. Optionally used to obtain additional browser information to facilitate risk-based decisioning.

Abbreviation	Descriptions
3DS Requestor	The initiator of the EMV 3-D Secure Authentication Request. For example, this may be a Merchant or a Digital Wallet requesting authentication within a purchase flow.
3DS Requestor App	An application on a Consumer Device that can process a 3-D Secure transaction using a 3DS SDK. The 3DS Requestor App is enabled through integration with the 3DS SDK.
3DS Requestor Environment	The 3DS Requestor-controlled components (3DS Requestor App, 3DS SDK, and 3DS Server) are typically facilitated by the 3DS Integrator. Implementation of the 3DS Requestor Environment will vary as defined by the 3DS Integrator.
3DS Requestor Initiated (3RI)	3-D Secure transaction initiated by the 3DS Requestor for the purposes of confirming that an account is still valid or for Cardholder authentication. The first main use case being recurrent transactions (TV subscriptions, utility bill payments, etc.) where the Merchant wants to perform a payment transaction to receive authentication data for each bill or a non-payment transaction to verify that a subscription user still has a valid form of payment. The second main use case is when the 3DS Requestor requests Decoupled Authentication as a method to authenticate the Cardholder.
3DS Requestor Website	Component that provides the website that requests Cardholder credentials (whether on file or entered by Cardholder).

Abbreviation	Descriptions
3-D Secure (3DS)	An e-commerce authentication protocol that enables the secure processing of payment, non-payment, and account confirmation card transactions.
Abandon	The act of a Cardholder leaving a transaction by use of the cancel action while in the process of a challenge. For example, using the cancel button in the App challenge UI.
Absent	Used in this specification to indicate that an element is absent when the name/value pair does not occur in the message. For example, element "firstName" is absent in the following JSON instance. `lastName: "Smith"`
Access Control Server (ACS)	A component that operates in the Issuer Domain, that verifies whether authentication is available for a Card number with/without a device type and authenticates specific Cardholders.
Access Control Server User Interface (ACS UI)	The ACS UI is generated during a Cardholder challenge and is rendered by the ACS within a Browser challenge window.
Acquirer	A business entity (can be a financial or non-financial institution) that establishes a contractual service relationship with a Merchant for the

Abbreviation	Descriptions
	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.
Acquirer Domain	Contains the systems and functions of the 3DS Requestor Environment and, optionally the Acquirer.
Attempts	In this specification, used to indicate the process by which proof of an authentication attempt is generated when payment authentication is not available. Support for Attempts is determined by DS.
Authentication	In the context of 3DS, the process of confirming that the person initiating an e-commerce transaction is entitled to use the Card.
Authentication Request Message (AReq)	An EMV 3DS message sent by the 3DS Server via the DS to the ACS to initiate the authentication process.
Authentication Response Message (ARes)	An EMV 3DS message returned by the ACS via the DS in response to an Authentication Request message.
Authentication Value (AV)	A cryptographic value generated by the ACS during authorisation processing, which will relay back to the authorisation system and used to validate the integrity of the authentication result. The AV algorithm is defined by the Payment System.

Abbreviation	Descriptions
Authorisation	A process by which an Issuer, or a processor on the Issuer's behalf, approves a transaction for payment.
Authorisation System	The systems and services through which a Payment System delivers online financial processing, authorisation, clearing, and settlement services to Issuers and Acquirers.
Bank Identification Number (BIN)	The first six digits of a payment card account number that uniquely identifies the issuing financial institution. Also referred to as Issuer Identification Number (IIN) in ISO 7812.
Base64	Encoding applied to the Authentication Value data element as defined in RFC 2045.
Base64url	Encoding applied to the 3DS Method Data, Device Information and the CReq/CRes messages as defined in RFC 7515.
Browser	In the context of 3DS, the browser is a conduit to transport messages between the 3DS Server (in the Acquirer Domain) and the ACS (in the Issuer Domain).
Card	In this specification, synonymous to the account of MyDebit payment card.
Card-Not-Present (CNP)	A payment card transaction transaction made where the Cardholder does not or cannot physically present the Card for a merchant's visual examination at the time that an order is given and payment effected.

Abbreviation	Descriptions
Cardholder	An individual to whom a Card is issued or who is authorised to use that Card.
Certificate	An electronic document that contains the public key of the certificate holder and which is attested to by a Certificate Authority (CA) and rendered not forgeable by cryptographic technology (signing with the private key of the CA).
Certificate Authority (CA)	A trusted party that issues and revokes certificates. Refers to DS Certificate Authority.
Challenge	The process where the ACS is in communication with the 3DS Client to obtain additional information through Cardholder interaction.
Challenge Flow	A 3DS flow that involves the ACS to obtain additional information through Cardholder interaction.
Challenge Request Message (CReq)	An EMV 3DS message sent by the 3DS SDK or 3DS Server where additional information is sent from the Cardholder to the ACS to support the Authentication process.
Challenge Reponses Message (CRes)	The ACS response to the CReq. It can indicate the result of the Cardholder authentication or, in the case of an App-based model, also signal that further Cardholder interaction is required to complete the authentication.
Consumer Device	Device used by a Cardholder such as a smartphone, laptop, or tablet that the Cardholder uses to conduct payment activities including authentication and purchase.

Abbreviation	Descriptions
Decoupled Authentication	Decoupled Authentication is an authentication method whereby authentication can occur independent from the Cardholder’s experience with the 3DS Requestor. The authentication method used for Decoupled Authentication is outside the scope of this specification, however one method could be a push notification to a banking app that completes authentication and then sends the results to the ACS. Decoupled Authentication is applicable to all Device Channels.
Device Channel	Indicates the channel from which a transaction originated. Either: • App-based (01-APP) • Browser-based (02-BRW) • 3DS Requestor Initiated (03-3RI)
Device Information	Data provided by the Consumer Device that is used in the Authentication process.
Digital Signature	An asymmetric cryptographic method whereby the recipient of the data can prove the origin and integrity of data; thereby protecting the sender of the data and the recipient against modification or forgery by third parties and the sender against forgery by the recipient.
Digital Wallet	A software component that allows a consumer to make an electronic payment with a financial instrument (such as MyDebit card) while hiding the low-level details of executing the payment protocol, including such tasks as entering an account number and providing shipping information and Cardholder identifying information.

Abbreviation	Descriptions
Directory Server (DS)	A server component owned and operated by PayNet in the Interoperability Domain; it performs several functions that include but not limited to authenticating the 3DS Server, routing messages between the 3DS Server and the ACS and validating the 3DS Server, the 3DS SDK, and the 3DS Requestor.
Directory Server ID (directoryServerID)	Registered Application Provider Identifier (RID) that is unique to the Payment System. RIDs are defined by the ISO 7816-5 standard.
Electronic Commerce Indicator (ECI)	Payment System-specific value provided by the ACS to indicate the results of the attempt to authenticate the Cardholder.

Empty	An element is empty if the field name is present, and the value is empty. For example, element "firstName" has no data in the following JSON instance.
	`firstName: "",`
	`lastName: "Smith"`

EMV	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.
EMV Payment Token	As defined in the EMV Tokenisation Specification, a surrogate value for a PAN that is a variable length, ISO/IEC 7812-compliant numeric

Abbreviation	Descriptions
	issued from a designated Token BIN or Token BIN Range and flagged accordingly in all appropriate BIN tables. A Payment Token passes basic validation rules of an account number, including the Luhn check digit. Payment Tokens do not have the exact same value as or conflict with a PAN.
EMVCo	EMVCo, LLC, a limited liability company incorporated in Delaware, USA. EMVCo exists to facilitate worldwide interoperability and acceptance of secure payment transactions.
Ends 3-D Secure Processing	In the 3DS processing flow, this indicates that no further processing as defined by this specification will be performed. It is the Merchant's preferences that an authorisation transaction may still be performed although it will happen without a successful 3DS authentication outcome.
Ends Processing	In the 3DS processing flow, this indicates that an error has been found by a specific 3DS component, which reports the error via the appropriate error message as defined in A.5.5 or RReq as defined in Table B.8 - EMV 3DS Protocol and Core Functions Specification The specific 3DS component reports the error to the component from which the erroneous message was received and may inform other components about the error and will stop further 3DS processing. The subsequent 3DS components in the authentication flow will still perform further execution of the received message with an error message to close the error situation. For an RReq, the sending component should expect back an RRes before stopping 3DS processing.

Abbreviation	Descriptions
FIDO Authenticator	An authentication entity that meets the FIDO Alliance’s requirements and which has related metadata. A FIDO Authenticator is responsible for user verification, and maintaining the cryptographic material required for the relying party authentication. For additional information, refer to: https://fidoalliance.org.
Frictionless	The process of authentication achieved without involves the ACS to obtain additional information through Cardholder interaction.
Frictionless Flow	A 3DS process flow of authentication achieved without involves the ACS to obtain additional information through Cardholder interaction.
Fully Qualified URL	Fully Qualified URL contains all the information necessary to locate a resource using the following format: scheme://server/path/resource. Example: https://server.domainname.com/acs/auth.html
Information Only	Information Only is a transaction status value, whereby the ACS acknowledges the 3DS Requestor’s preference to not challenge on the transaction since the data sent was only for informational purposes.
Interaction Counter	The number of interactions for each transaction is tracked by the ACS and sent with the RReq to the DS. Used by the ACS to set a maximum number of Cardholder interactions as determined by the selected Challenge Flow and security requirements to allow an appropriate number of Cardholder retries without going beyond a pre-set maximum.
Interoperability Domain	Interoperability Domain contains the DS systems which facilitates the transfer of information between the Issuer Domain and Acquirer

Abbreviation	Descriptions
	Domain systems.
Issuer	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.
Issuer Domain	Contains the systems and functions of the Issuer and its customers (Cardholders).
JavaScript Object Notation (JSON)	An open standard format that uses human-readable text to transmit data objects consisting of attribute-value pairs. It is typically used to transmit data between a server and web application. Refer to Appendix 7.8.1 for RFC references.
Key	In cryptography, the Key is a piece of information (a parameter) needed to encrypt and/or decrypt a value.
Key Management	The handling of cryptographic Keys and other security parameters during the entire lifetime of the Keys, including generation, storage, entry and use, deletion or destruction, and archiving.
MAC	Message Authentication Code. A symmetric (secret key) cryptographic method that protects the sender and recipient against any modification and forgery of data by third parties.
Merchant	A company, entity, statutory or government body that contracts with an Acquirer and/or PayNet to accept MyDebit Secure payments. Manages the online CNP purchase (e-commerce) experience with the

Abbreviation	Descriptions
	Cardholders, obtains Cards information and then transfers control to the 3DS Server, which conducts payment authentication.
Message Category	Indicates the category of the EMV 3DS message. Either: • Payment (01-PA); or • Non-Payment (02-NPA).
Message Version	Refers to the protocol version that will be used by all components to process the 3DS transaction. Message Version is always consistent across all 3DS protocol messages for a specific transaction.

Missing	An element is missing either if it is absent (that is the name/value pair does not occur in the message) or if the field name is present, but the value is empty. For example, element "firstName" has no data in both of the following JSON instances.
	Example of empty field name present and value empty:
	`firstName: "",`
	`lastName: "Smith"`
	`Example of absent name/value pair:`
	`lastName: "Smith"`

Abbreviation	Descriptions
Name/value Pair (NVP)	A simple class encapsulating an attribute/value pair.
Native	Refers to the original method for a device display, utilising its own APIs.

Null	An element is Null if the field name is present, and the value is null. For example, element "firstName" has null in the following JSON instance.
	`firstName: null,`
	`lastName: "Smith"`

One-Time Passcode/Password (OTP)	A passcode (password) that is only be used once for one login session or transaction on a computer system or other digital device. Time-based OTP which its validity is limit for a certain amount of time is recommended.
Out-of-Band (OOB)	A Challenge activity that is completed outside of, but in parallel to, the 3DS flow. The final CReq is not used to carry the data to be checked by the ACS but signals only that the authentication has been completed. ACS authentication methods or implementations are not defined in the 3DS specification.
Participants	The appointed entity and relevant financial institution, non- financial institution, statutory or government body that meet the eligibility requirements specific to MyDebit to participate in the MyDebit Scheme.

Abbreviation	Descriptions
	Refer to Operational Procedures for MyDebit - PART III MEMBERSHIP and has entered a contractual service relationship to accept, authenticate and process transactions in the Program.
Payment System	Payment System here is referring to PayNet MyDebit, which defines the Program participation rules, operating rules and the requirements for Card issuance and Merchant acceptance.
PayNet Authentication Value	A specific value generated by PayNet's DS after Authentication has been attempted or completed.
PayNet Issuer Authentication Value	A specific value generated and provided by the Issuer's ACS after authentication has been attempted or completed. Authentication Value may be used to provide proof of authentication.
Preparation Request Message (PReq)	A 3DS message sent from the 3DS Server to the DS to request the ACS and DS Protocol Version(s) that correspond to the DS Card ranges as well as an optional 3DS Method URL to update the 3DS Server's internal storage information.
Preparation Response Message (PRes)	Response to the PReq message that contains the DS Card Ranges, active Protocol Versions for the ACS and DS and 3DS Method URL so that updates can be made to the 3DS Server's internal storage.
Private Key	Part of an asymmetric cryptographic system. The Key that is kept secret and known only to an owner.

Abbreviation	Descriptions
Proof of authentication attempt	Refer to Attempts.
Protocol Version	Refers to the version of the EMV 3DS specification that the component supports. The Protocol Version referring herewith is the EMV 3DS specification version 2.2.0.
Public Key	This is part of an asymmetric cryptographic system. The Key which is disseminated widely and made available to Participants via a publicly accessible repository or directory.
Public Key Pair	Two mathematically related keys—a public key and a private key—that are used with a public key (asymmetric) cryptographic algorithm to permit the secure exchange of information without the necessity for a secure exchange of a secret.
Results Request Message (RReq)	Message sent by the ACS via the DS to transmit the results of the authentication transaction to the 3DS Server.
Results Response Message (RRes)	Message sent by the 3DS Server to the ACS via the DS to acknowledge receipt of the Results Request message.
Registered Application Provider Identifier (RID)	Registered Application Provider Identifier (RID) is unique to a Payment System. RIDs are defined by the ISO 7816-5 standard and are issued by the ISO/IEC 7816-5 registration authority. For details on ISO 7816-5, refer to Appendix 7.8.2. RIDs are 5 bytes.

Abbreviation	Descriptions
Secret Key	A key used in a symmetric cryptographic algorithm such as DES which, if disclosed publicly, would compromise the security of the system.
Transport Layer Security (TLS)	A cryptographic protocol developed by the IETF (Internet Engineering Task Force) to confidentially transmit information over open networks, such as the Internet. Refer to Appendix 7.8.1 for RFC references.
Uniform Resource Locator (URL)	Address scheme for pages on the World Wide Web usually in the format http://www.example.com or https://www.example.com.
Universally Unique Identifier (UUID)	Identifier standard used in software construction. In its canonical form, a UUID is represented by 32 lowercase hexadecimal digits, displayed in five groups separated by hyphens, in the form 8-4-4-4-12 for a total of 36 characters (32 alphanumeric characters and four hyphens). Refer to Appendix 7.8.1 for RFC references.
Whitelisting	In this specification, the process of an ACS enabling the Cardholder to place the 3DS Requestor on their trusted beneficiaries list.
X.509	Certificate format as defined in RFC 4158

Overview of MyDebit Secure Program

Malaysia debit cards are issued as dual-brand cards with MyDebit as one of the two card brands displayed on the front of the card. For e-commerce, CNP transaction processing exists in two stages:

Authentication, where E3DS applies; and

Authorization, where financial messages are exchanged via the ISO 8583 messaging standard. On both stages, messages need to be correctly routed to the relevant card network, so as not to confuse the consumers that may result in abandonment of the shopping cart.

Benefits

The volume of CNP transactions is growing at a rate 2 to 3 times as fast of Card-Present transactions. The volume of CNP transactions that are conducted via a mobile device has overtaken that of a traditional personal computer environment.

Benefits to Consumers:

- Increased trust and confidence in the e-commerce environment where the online purchases are made, knowing that the transactions have been conducted in a secured 3DS environment
- Streamlined verification process to provide seamless experience during checkout

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

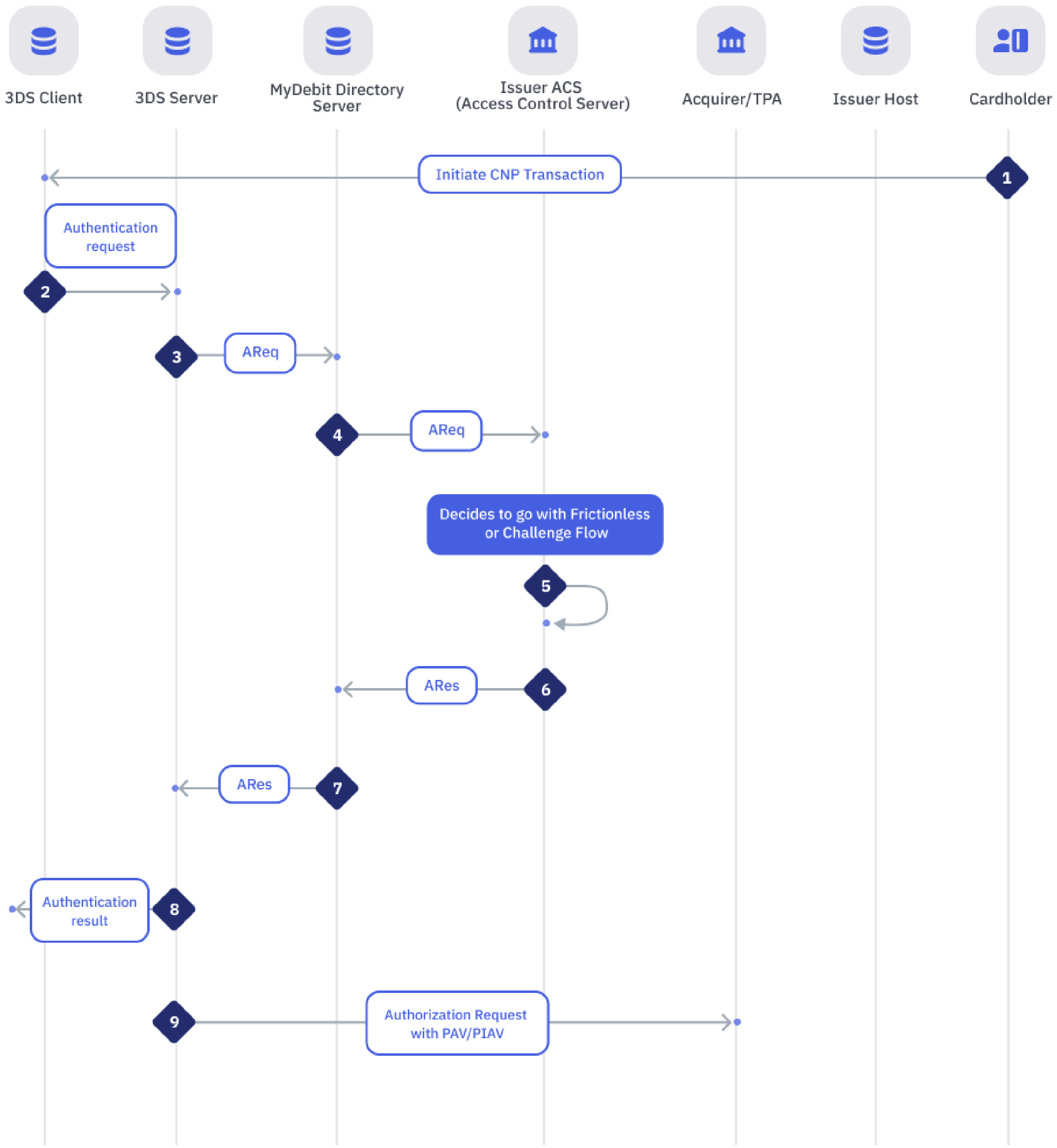
Benefits to Acquirers, Merchants, and Merchant Processors:

- 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

Frictionless Flow

The Frictionless Flow initiates a 3-D Secure Authentication Flow and consists of an AReq message and an ARes message. The Frictionless Flow does not require further Cardholder interaction to achieve a successful Authentication and complete the 3-D Secure Authentication process.

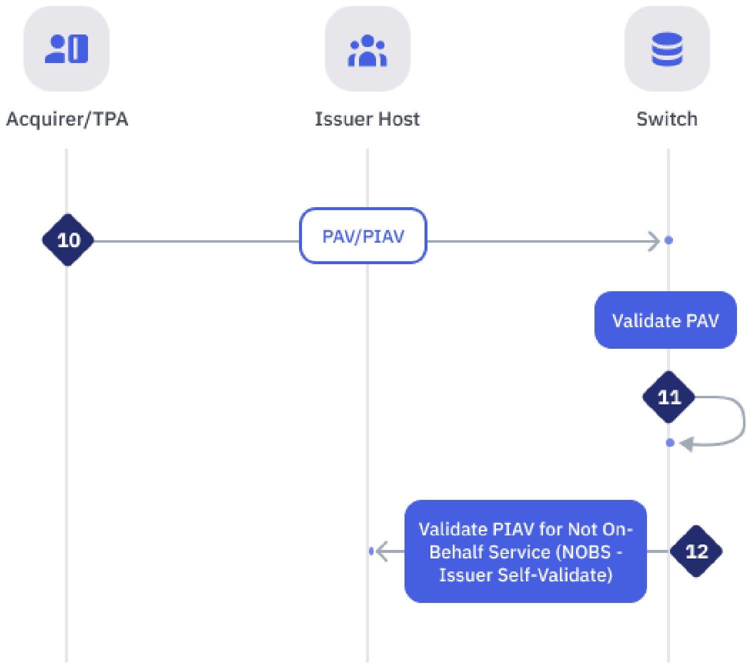
CNP Authentication : Frictionless Flow Steps 1-9


3DS Client
3DS Server
MyDebit Directory Server
Issuer ACS (Access Control Server)
Acquirer/TPA
Issuer Host
Cardholder
1
Initiate CNP Transaction
Authentication request
2
3
AReq
4
AReq
Decides to go with Frictionless or Challenge Flow
5
ARes
6
ARes
7
Authentication result
8
9
Authorization Request with PAV/PIAV

Step	Sender	Receiver	Process
1	Cardholder	3DS client	Initiate CNP transaction
2	3DS Client	3DS Server	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.
3	3DS Server	MyDebit Directory Server	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.
4	MyDebit Directory Server	Issuer ACS [Access Control Server]	DS then forwards the AReq message to the appropriate ACS.
5	Issuer ACS [Access Control Server]	Issuer ACS [Access Control Server]	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.
6	Issuer ACS [Access Control Server]	MyDebit Directory Server	In response to the AReq message, the ACS returns an ARes message to the DS. Before returning the response, the ACS evaluates the data provided in the AReq message. Issuer subscribe to On-Behalf Service, • if ECI 15 is returned, DS will generate PAV and return in ARes message.

Step	Sender	Receiver	Process
			• if ECI 16 is returned, DS will generate PAV and return in ARes message. Issuer not subscribe to On-Behalf Service, • if ECI 15 is returned, ACS will need to generate PIAV and return in ARes message. • if ECI 16 is returned, DS will generate PAV and return in ARes message.
7	MyDebit Directory Server	3DS Server	DS then forwards the ARes message together with PAV or PIAV to the initiating 3DS Server.
8	3DS Server	3DS Client	The 3DS Server communicates the result of the ARes message to the 3DS Requestor Environment which then informs the Cardholder.
9	3DS Server	Acquirer/TPA	Callback to original request from acquirer/TPA, with PAV or PIAV.

CNP Authentication : Frictionless Flow Steps 10-12

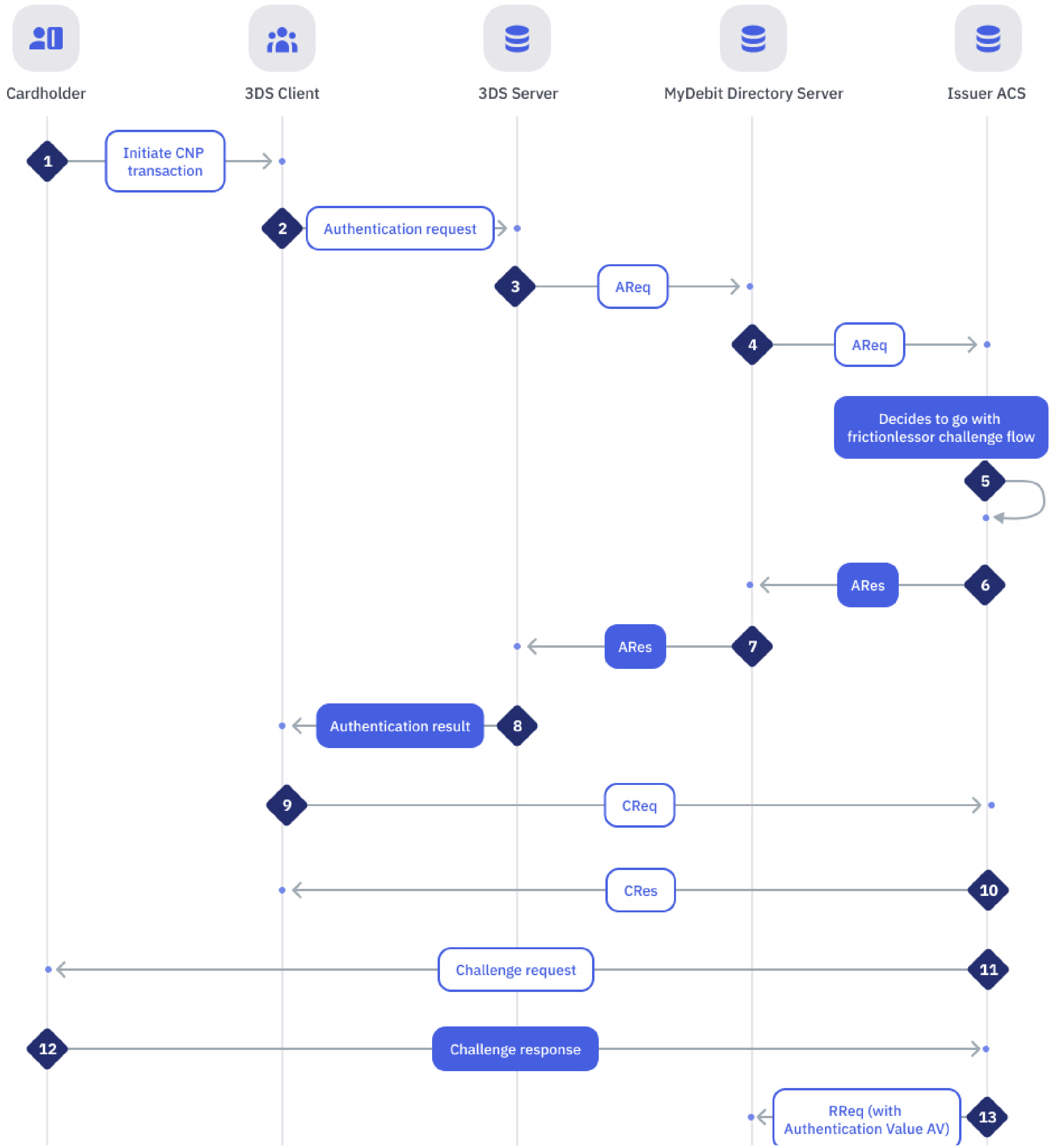

Acquirer/TPA
Issuer Host
Switch
10
PAV/PIAV
Validate PAV
11
Validate PIAV for Not On-Behalf Service (NOBS - Issuer Self-Validate)
12

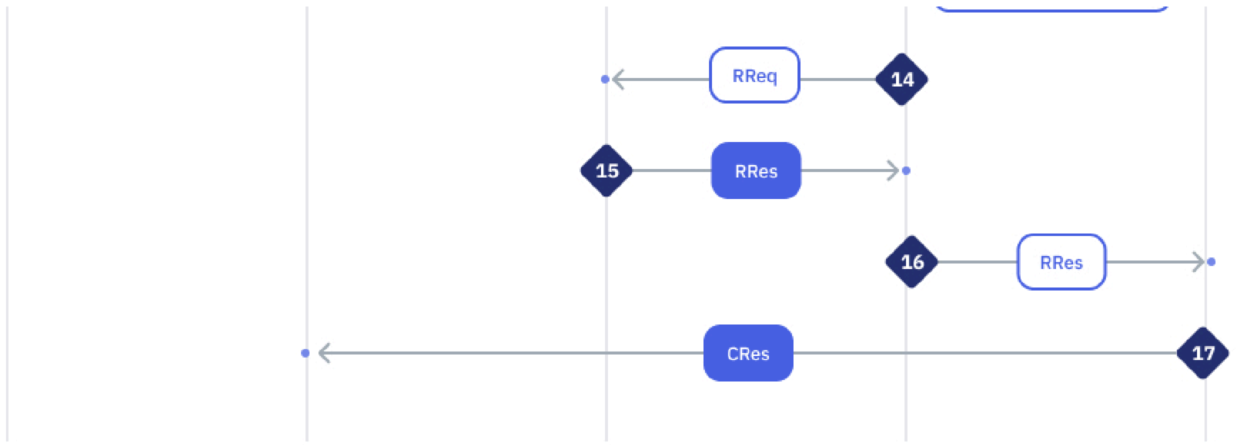
Step	Sender	Receiver	Process
10	Acquirer/TPA	MyDebit Switch	ISO8583 PAV + PIAV + PAN. PAN = Primary Account Number The acquirer/TPA communicates with MyDebit switch. The acquirer/TPA sends an authorization request along with the authentication status and details to MyDebit switch.
11	MyDebit Switch	MyDebit Switch	Validate PAV if PAV exists.
12	MyDebit Switch	Issuer Host	Validate PIAV for not On-Behalf Service [NOBS - Issuer Self-Validate only for ECI 15]

Challenge Flow

In addition to the AReq and ARes messages that comprise the Frictionless Flow, the Challenge Flow consists of CReq, CRes, RReq, and RRes messages. If the ACS determines that further Cardholder interaction is required to complete the Authentication process, the Frictionless Flow transitions into the Challenge Flow. For example, a Challenge may be necessary because the transaction is deemed high-risk, i.e. above a pre-determined threshold, or requires a higher level of Authentication due to country mandates (or regulations). 3DS Requestor may decide whether to proceed with the Challenge, or to terminate the 3-D Secure Authentication process.

CNP Authentication : Challenge Flow Steps 1 - 17


Cardholder
3DS Client
3DS Server
MyDebit Directory Server
Issuer ACS
1
Initiate CNP transaction
2
Authentication request
3
AReq
4
AReq
Decides to go with frictionlessor challenge flow
5
6
ARes
7
ARes
8
Authentication result
9
CReq
10
CRes
11
Challenge request
12
Challenge response
13
RReq (with Authentication Value AV)



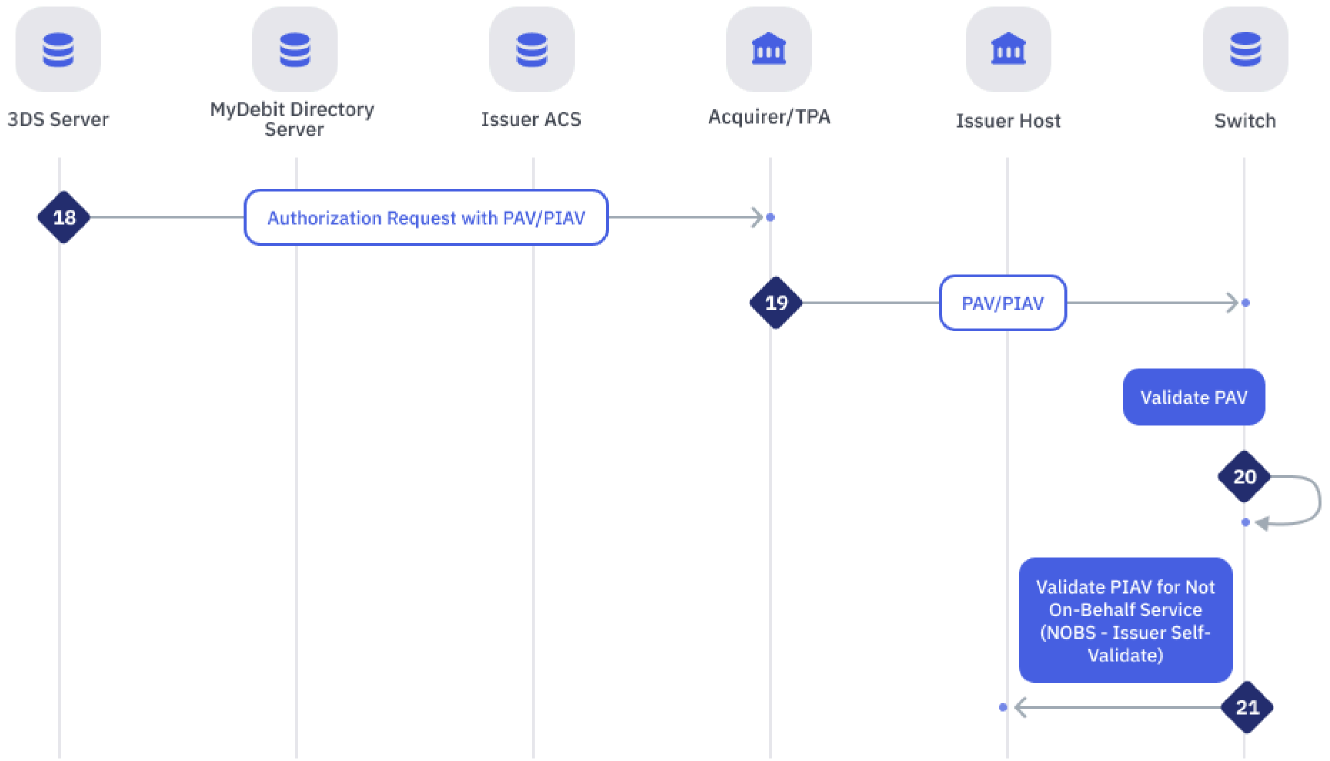
Step	Sender	Receiver	Process
1	Cardholder	3DS client	Initiate CNP transaction
2	3DS Client	3DS Server	Within the 3DS Requestor Environment, the necessary 3-D Secure information is gathered and provided to the 3DS Server for inclusion in the AReq message.
3	3DS Server	MyDebit Directory Server	Using the 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.
4	MyDebit Directory Server	Issuer ACS [Access Control Server]	DS then forwards the AReq message to the appropriate ACS.

Step	Sender	Receiver	Process
5	Issuer ACS [Access Control Server]	Issuer ACS [Access Control Server]	ACS evaluates the data provided in the AReq message. If the ACS determines that the transaction requires additional authentication, Challange Flow will be applied.
6	Issuer ACS [Access Control Server]	MyDebit Directory Server	In response to the AReq message, the ACS returns an ARes message to the DS
7	MyDebit Directory Server	3DS Server	DS then forwards the ARes message to the initiating 3DS Server.
8	3DS Server	3DS Client	The 3DS Server communicates the result of the ARes message to the 3DS Requestor Environment which then informs the Cardholder. Further Cardholder interaction is required to complete the authentication.
9	3DS Client	Issuer ACS [Access Control Server]	The 3DS Client initiates a CReq message based on information received in the ARes message. A CReq message is sent to the ACS URL received from the ARes message. Next, the ACS receives the CReq message and interfaces with the 3DS Client to facilitate Cardholder interaction.
10	Issuer ACS [Access	3DS Client	The ACS returns a CRes message to the 3DS Client. Based on the CRes obtained from the ACS,

Step	Sender	Receiver	Process
	Control Server]		the 3DS Client displays the challenge-specific screens for the Cardholder to enter their authentication data.
11	Issuer ACS [Access Control Server]	Cardholder	Challenge Request e.g. OTP
12	Cardholder	Issuer ACS [Access Control Server]	Challenge Response e.g.
13	Issuer ACS [Access Control Server]	MyDebit Directory Server	The ACS sends an RReq message that can include the PAV/PIAV to the DS.
14	MyDebit Directory Server	3DS Server	DS then routes the RReq message to the appropriate 3DS Server using the 3DS Server URL received from the AReq message.
15	3DS Server	MyDebit Directory Server	The 3DS Server receives an RReq message and in response, returns an RRes message to the DS
16	MyDebit Directory	Issuer ACS [Access	DS then routes the message to the ACS

Step	Sender	Receiver	Process
	Server	Control Server]	
17	Issuer ACS [Access Control Server]	3DS Client	The ACS sends the final CRes message to the 3DS Client to indicate the result of the authentication.

CNP Authentication : Challenge Flow Steps 18 - 21


3DS Server
MyDebit Directory Server
Issuer ACS
Acquirer/TPA
Issuer Host
Switch
18
Authorization Request with PAV/PIAV
19
PAV/PIAV
Validate PAV
20
Validate PIAV for Not On-Behalf Service (NOBS - Issuer Self-Validate)
21

Step	Sender	Receiver	Process
18	3DS Server	Acquirer/TPA	Callback to original request from acquirer/TPA, with PAV or PIAV
19	Acquirer/TPA	MyDebit Switch	ISO8583 PAV + PIAV + PAN. PAN = Primary Account Number The acquirer/TPA communicates with MyDebit switch. The acquirer/TPA sends an authorization request along with the authentication status and details to MyDebit switch.
20	MyDebit Switch	MyDebit Switch	Validate PAV if PAV exists
21	MyDebit Switch	Issuer Host	Validate PIAV for not On-Behalf Service [NOBS - Issuer Self-Validate only for ECI 15]

MyDebit Secure Certificate Authority

All digital Certificates will be generated/signed under the Program root certificate. These Certificates include:

- TLS client and server certificates used in the establishment of the communication channels between
    - the 3DS Server and the DS
    - 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 and/or 3DS SDK

Table below is the Certificates involved in an EMV 3DS environment

Certificate Name	Certificate Authority	Stored Location	Usage
MyDebit Secure CA Root Certificate	PayNet	ALL 3DS components	Validation of all Certificates issued under the same PayNet Program root
3DSS Client Certificate	PayNet	3DS Client3DS Client	The consumer-facing component allowing consumer interaction with the 3DS Requestor for initiation of the EMV 3-D Secure protocol.
3DS Client3DS Client	PayNet	3DS Client3DS Client	The consumer-facing component allowing consumer interaction with the 3DS Requestor for initiation of the EMV 3-D Secure protocol.
Commercial Server Certificate (for 3DS Method)	Commercial CA	ACS	TLS channel encryption between browser and ACS for 3DS Method