Debit Technical Working Group

U.S. Debit EMV Technical Proposal

Version 1.3

Version History:

- Version 1.3, April 2015 – U.S. Common Debit Contactless Addendum added
- Version 1.2, April 2014 – Initial publication

NOTES AND INFORMATION DISCLOSURE:

This document has been prepared by the EMV Migration Forum Debit Technical Working Group. The purpose of the document is for Forum members to review and consider the viability of the proposal herein from a technical perspective, business arrangements notwithstanding. The proposal sets forth a functional description of a possible approach for a technical solution when the U.S. common debit AID is selected for online PIN, No CVM and Signature, which should not be considered the only approach. The document provides only a high-level description of the technical solution, and stakeholders interested in implementing an actual solution consistent with the proposal in their own environments will therefore need to develop their own detailed specifications. Accordingly, consideration or validation of this proposal from a technical perspective does not and cannot be construed to obligate or commit any EMV Migration Forum member or the Forum to adopt the proposal or any particular solution or approach described herein. To the best of the knowledge of the authors, this document does not contain any confidential and proprietary technology or information. The proposal described in this document is based on input from the participants in the Working Group and is intended to be consistent with publicly available and royalty free EMV specifications published on www.emvco.com. All attempts have been made to present the approach and any market details described herein from an independent and neutral point of view.

About the EMV Migration Forum

The EMV Migration Forum is a cross-industry body focused on supporting the EMV implementation steps required for global and regional payment networks, issuers, processors, merchants, and consumers to help ensure a successful introduction of more secure EMV chip technology in the United States. The focus of the Forum is to address topics that require some level of industry cooperation and/or coordination to migrate successfully to EMV technology in the United States. For more information on the EMV Migration Forum, please visit http://www.emv-connection.com/emv-migration-forum/.

TABLE OF CONTENTS

1 Introduction

Since the inception of the EMV Migration Forum (the Forum), one of its most discussed topics has been the development of a technical solution to implement EMV technology in the U.S. debit market in a manner that is compliant with Regulation II of the Durbin Amendment to the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ("Reg II"). An EMV Migration Forum debit working group diligently gathered facts and consensus-based preferences from participating industry stakeholder groups in an effort to drive forward a technological path for implementing EMV debit in the US. Subsequently, a technical sub-group called "The tag group" presented three different solution proposals and these were under review. Just shortly after this, a court ruling (the "Judge Leon ruling") against the Federal Reserve Board, and the subsequent appeal of that ruling, brought the EMV Migration Forum's efforts to come to a consensus on a viable technical approach for a U.S. EMV debit solution to a stand-still. In an attempt to move forward despite the uncertainty of regulatory requirements in light of the Judge Leon ruling, the EMV Migration Forum Steering Committee formed a new EMV Debit Technical Working Group to help restart discussions regarding technologically viable U.S. EMV debit solutions.

The primary goal of this paper is to summarize the relevant information gathered within the EMV Migration Forum since September 2012, particularly the considerations addressed by the new EMV Debit Technical Working Group, and propose a source-agnostic set of baseline technical specifications for a U.S. EMV debit solution that is intended to be consistent with applicable technical and regulatory requirements and provide a viable technological approach for moving forward (the "Solution").

Accordingly, the Solution described in this document is intended as a model, or framework, capable of satisfying the specifications and requirements noted above, and as a result, serving as the basis for one or more technological solutions to be developed based on the Offered Solutions (defined below) or other technology.

The EMV Migration Forum is not in a position to mandate adoption of or compliance with the Solution, or any of the Offered Solutions. Rather, it seeks acknowledgement by interested stakeholders and EMV Migration Forum members that the Solution outlined in this document is viable from a technological perspective, business arrangements notwithstanding.

The Solution is based entirely on EMV chip technology with no proprietary defined data elements or logical process steps between the card and the acceptance device.

The Solution is also based on the existence of a set of messages that are transmitted between and through the terminal, acquirer, payment network, related processors and issuer. These messages are used to seek approval of the transaction and provide the issuer's decision. These messages are defined by the various parties to the transaction and may require modification above and beyond those described in Book 4 of the EMV specifications. Several acquirers and payment networks have already issued EMV amendments to the message specifications for these terminal and network level interfaces. It should be further noted that some have already certified the network interfaces necessary to meet the April 2013 mandates.

The main aspect of the Solution is that once the U.S. Debit AID is selected by the merchant, the Solution will enable flexible CVM selection that doesn't affect the acceptance device's EMV kernel certification and accommodates foreseeable future routing requirements set by the industry and/or regulators.

As part of the Solution, the U.S. common debit AID would be shared across U.S. debit networks and would be for domestic use. The geographical scope of the common debit AID would apply to all U.S. states, territories and protectorates as recognized by Reg II. For further details on implementation

considerations for card, POS and ATM configuration as it relates to the U.S. territories and protectorates, please see Section 6.1.1 .

The Solution described in the document is focusing on contact transaction processing. In principle it may be compatible with a contactless transaction when implemented on a dual interface EMV card or a mobile device, but at this stage this is outside the scope of this document. More work is required to describe recommendations ensuring successful contactless multi-network transaction processing. EMV functionality of a contactless POS device is often optimized for speed, which may present challenges with multi-AID selection. In addition, there is a need to further analyze the requirements for international interoperability of a contactless enabled payment device – i.e., proper configuration of PPSE (Proximity Payment System Environment). If planning to issue contactless-enabled U.S. debit EMV cards at present, as a financial institution, please seek guidance to ensure Reg II compliance is met in the implementation. The technical work group will continue to work on addressing contactless acceptance for U.S. common debit AID.

The Solution should be "future proof" as defined in Section 2.1 according to merchant requirement [M3], allowing support of possible future regulatory requirements of routing both PIN and signature transactions over two or more non-affiliated networks.

U.S. debit EMV acceptance at an ATM device will be described by the EMV Migration Forum ATM Working Committee.

1.1 Assumptions

The Solution assumes that all debit networks that wish to be represented in a Single Common AID on a card are in fact represented in the Single Common AID. Whether or not a given debit network is so represented depends on business arrangements between the debit network and other industry stakeholders; such business arrangements are outside the scope of this proposal and the EMV Migration Forum. Discussions regarding these business arrangements are ongoing between independently-acting industry constituents, and the document does not suggest that they have been resolved. Issuers and acquirers should consult with their respective network partners prior to any debit implementations.

2 Solution Expectations

The EMV Debit Technical Working Group has been tasked to propose a Solution that satisfies all of the following industry stakeholder group expectations.

2.1 Merchants

[M1] Merchant's terminal should be able to select a single common debit AID to facilitate multi-network debit transaction routing.

[M2] The Solution should satisfy current regulatory requirements for the issuer to offer at least two unaffiliated network routing choices.

[M3] The Solution should be "future proof" – i.e., it should allow support of possible future regulatory changes requiring routing of both PIN and signature transactions over two or more non-affiliated networks. Changes to implement two or more signature debit network routing should not require a merchant to make additional software changes to their point-of-sale (POS) infrastructure.

[M4] The Solution should minimize the cost of deployment by requiring minimal to no deviation from the EMV specifications, and should minimize or eliminate any terminal kernel changes.

[M5] Merchants should not need to connect to the host to make the application selection decision. For performance reasons all decisions should be available locally at the POS as they are today.

2.2 Issuers

[I1] The Solution should enable issuers to fulfill present regulatory requirements to satisfy [M2].

[I2] Issuers should be able to switch networks serving the U.S. market without reissuing cards already in the field.

[I3] Issuers should be able to switch networks serving the U.S. market without making any script changes of cards already in the field.

[I3] Issuers should be able to satisfy foreseeable future regulatory changes without reissuing cards in the field.

[I4] The Solution should minimize the cost and complexity of the EMV chip embedded in the cards.

[I5] In the case where issuers use their own host for transaction approval/process, the Solution should allow issuers to approve transactions with minimal complexity at the host while maintaining risk management and the security of the EMV transaction online authentication and approval.

2.3 Payment Networks

[P1] The Solution should enable payment networks and issuers to employ any form of cardholder verification described in the EMV specifications.

[P2] The Solution should enable payment networks to employ any method of card authentication described in the EMV specifications.

[P3] The Solution should enable payment networks and issuers to support any method of transaction authorization described in the EMV specifications.

3 Transaction Flow – Solution Description

3.1 Offered U.S. Common Debit Solutions

From a purely technological perspective, the Solution proposed can be implemented on any of the three U.S. common debit solutions currently offered in the marketplace (the "Offered Solutions"), which are as follows:

- MasterCard international AID + Maestro U.S. common debit AID based on MasterCard M/Chip 4 or Advance and PayPass based EMV application.
- Any AID + DNA U.S. common debit AID based on any number of DNA approved EMV compliant application(s)
- Visa international AID + Visa U.S. common debit AID based on VISA VIS 1.4/1.5 and VCPS 2.1 based EMV application

In practice, however, whether the implementation of a given Offered Solution in a given instance will satisfy the expectations specified in Section 2 will ultimately depend on business arrangements outside the scope of this document and the EMV Migration Forum. For additional information regarding a given Offered Solution, interested parties should contact the applicable provider.

The details described in this proposal as part of the Solution do not use any proprietary feature of the above three payment application Offered Solutions, but only rely on common EMV functionality available in all of the supported applications.

To satisfy [M1 and I4], the proposed Solution assumes the use of a single common debit AID on a given card. As a corollary, it is noted that as part of the Solution, different cards may use different common debit AIDs, and there is no assumption that there will be only one common debit AID across the industry.

From a technological perspective, the Solution enables the merchant to route transactions to all networks supported by the issuer, by selecting the U.S. debit common AID on the card. Different issuers may support different networks, and accordingly, different networks may be available to different merchants depending on which networks issuers support.

3.2 Cardholder Verification

3.2.1 PIN

Online PIN is the primary CVM used in single message (SMS) debit transactions today. Many issuers support more than one PIN debit network. Online PIN functionality on an EMV card is no different than the way it is supported today with mag-stripe cards.

Due to the fact that this method is widely used today and there is an infrastructure and associated experience, it is likely that online PIN will continue to be used as the primary CVM method for the U.S. common debit AID. Therefore it is likely that U.S. debit networks supporting a U.S. common debit AID would want to be able to support this CVM method.

Offline PIN is outside the scope of this document.

3.2.2 No CVM

"No CVM" is an important option for low value transactions often performed with a debit card at convenience stores, automated ticketing machines, vending machines, fast food restaurants and many other merchant categories.

For the best user experience and fast transaction processing of low value transactions, a U.S. debit EMV card should support "No CVM".

The proposed Solution describes how merchants can facilitate a "No CVM" transaction (see diagram in Section 3.3) independent of the risk management decisions each network will make in defining their unique "No CVM" limit(s). The goal is to support "No CVM" transactions while ensuring there are no impacts or changes in the future required to the card, POS solution or network message specification.

Two scenarios of "No CVM" processing are described below:

- PIN preferring merchants. PIN entry message is always presented to the consumer regardless of the amount of the transaction. If a consumer opts out of PIN, the merchant will initiate what this Solution refers to as a "No PIN" transaction. The amount of the transaction, as well as the full primary account number (PAN), will be used to select the merchant's chosen debit network that supports this amount as either "No CVM" or signature. The merchant's decision to route over a network supporting "No CVM" vs. signature is a choice they can make based on various business rules and performance of the transaction processing as established by the issuer and the network.
- Fast transaction preferring merchants. Per the description above, merchants whose primary goal is to achieve fast customer service may choose to use "No CVM" as a primary method by establishing a lowest common "No CVM" limit value over all the supported networks. As such, if the transaction amount is below this limit, the merchant will skip PIN entry and use "No CVM" option directly. If the amount is above the lowest common "No CVM" limit, the merchant will have a choice to either:
    - Prompt for PIN first to facilitate higher value transactions using PIN; or prompt for signature depending on issuer instruction and support of network capabilities.
    - Not to prompt for PIN even if the amount is above the lowest common "No CVM" limit. In this case, the transaction will be sent to the acquirer and can complete as "No CVM" over a network that supports a higher limit or a network that will have indicated a signature is required.

3.2.3 Signature

The proposed Solution describes two alternatives for CVM processing logic, where the decision to use signature or "No CVM" is made by the store/acquirer host based on the chosen network transaction processing rules – see Section 3.3. To ensure future-proofing and flexibility of the CVM processing, the terminal should receive a response indicating if signature is required once an approval has been received. For more details on this process please see Section 5.1.

3.3 Future-proofing Debit EMV in the Common AID

The EMV Debit Technical Working Group includes representation from several different networks and a considerable amount of dialog has occurred highlighting differences regarding potential approaches for supporting signature transactions. The group's goal was to achieve a consensus using a single solution. However, as noted above, two alternate conceptual solution frameworks have emerged for CVM processing logic, as further described in Sections 3.3.1 and 3.3.2 below.

Either of these two CVM processing approaches provides both merchants and issuers a "future proof" solution, as outlined in Section 1, to implement host-managed CVM processing.

Neither alternative presents a constraint to support either single or dual message processing; however, merchants should work with their acquirer/processor on implementing these routing options.

3.3.1 Common AID with PIN and No CVM

To satisfy merchant expectations, and in particular [M1] and [M3], the CVM processing logic described in this Section 3.3.1 ("Alternate 1") is designed to provide merchants with a flexible decision-making approach for signature transactions at the merchant's store/acquirer host.

It has been identified that various networks have different capabilities and rules. These differences make CVM selection at the POS device impractical. At the time of processing of an EMV transaction at the POS, the terminal may not know its available routing choice. Having the option to identify a transaction as a "No CVM" or signature at the merchant's store/acquirer host instead allows this decision to be made only after the host takes into consideration all routing choices available.

In addition to merchant flexibility in deciding routing at the host, Alternate 1 recommends having a minimal set of CVMs listed on the card, which will also allow issuers to better adjust their risk management while providing updates to their respective routing tables and not impacting cards already issued in the field.

Under Alternate 1, the recommended CVM list on the card would only facilitate a decision between a PIN or a "No PIN" transaction, while the signature/"No CVM" processing has been removed from the interaction between the card and the terminal.

This Alternate preserves the ability of a debit network to service transactions with different "No CVM" limits.

Under Alternate 1, the recommended minimum CVM list on the card is as follows:

Online PIN – for ATM and POS use with or without cash back

No CVM – for POS use, facilitating signature and "No CVM" transactions without cash back

The flow chart provided in Figure 3.1 below presents further details on how the processing would work under Alternate 1.

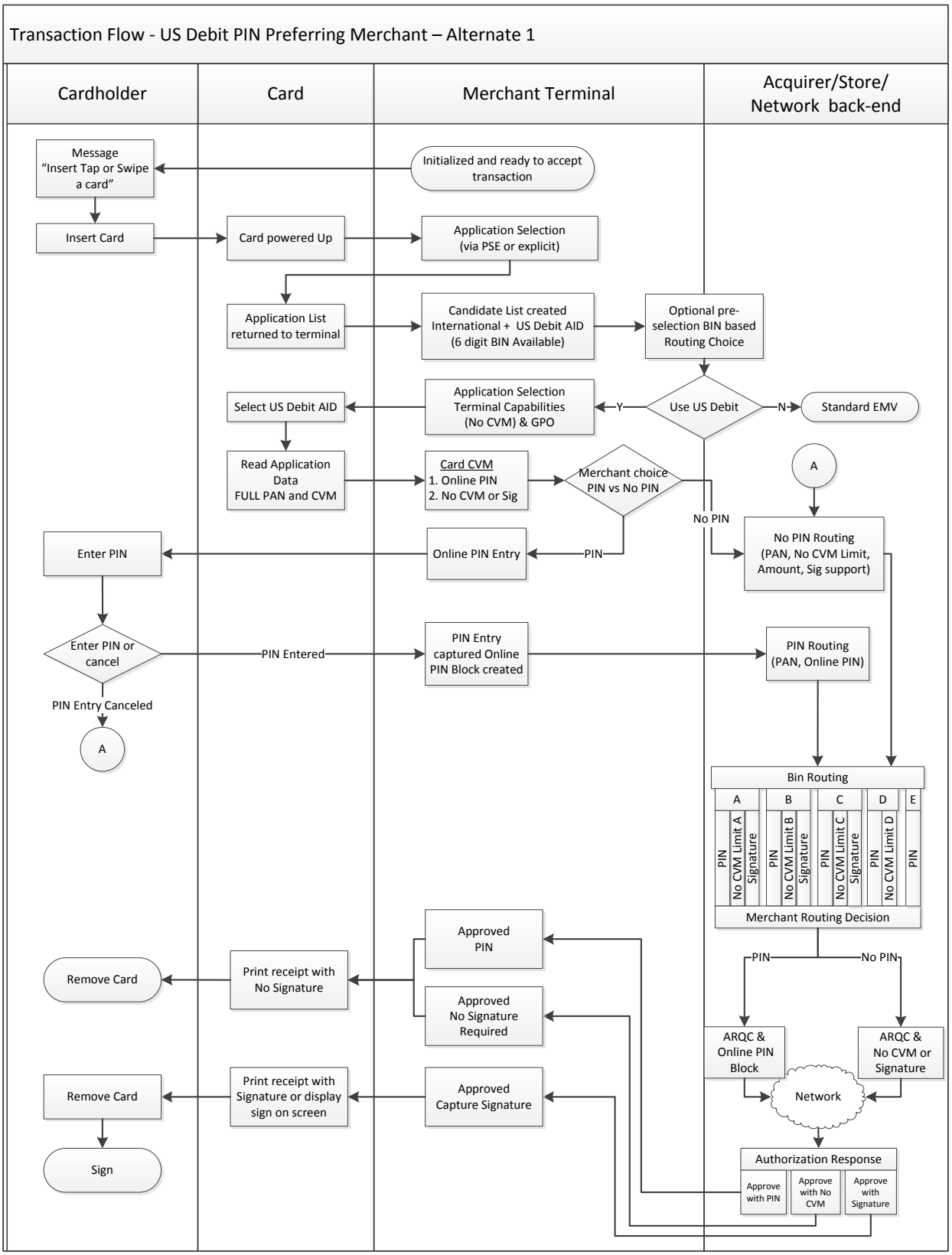

Transaction Flow - US Debit PIN Preferring Merchant – Alternate 1
Cardholder
Card
Merchant Terminal
Acquirer/Store/ Network back-end
Message "Insert Tap or Swipe a card"
Initialized and ready to accept transaction
Insert Card
Card powered Up
Application Selection (via PSE or explicit)
Application List returned to terminal
Candidate List created International + US Debit AID (6 digit BIN Available)
Optional pre-selection BIN based Routing Choice
Select US Debit AID
Application Selection Terminal Capabilities (No CVM) & GPO
Y
Use US Debit
N
Standard EMV
Read Application Data FULL PAN and CVM
Card CVM
1. Online PIN
2. No CVM or Sig
Merchant choice PIN vs No PIN
A
No PIN
Enter PIN
Online PIN Entry
PIN
No PIN Routing (PAN, No CVM Limit, Amount, Sig support)
Enter PIN or cancel
PIN Entered
PIN Entry captured Online PIN Block created
PIN Routing (PAN, Online PIN)
PIN Entry Canceled
A
Bin Routing
A
B
C
D
E
PIN
No CVM Limit A
Signature
PIN
No CVM Limit B
Signature
PIN
No CVM Limit C
Signature
PIN
No CVM Limit D
PIN
Merchant Routing Decision
PIN
No PIN
Approved PIN
Remove Card
Print receipt with No Signature
Approved No Signature Required
ARQC & Online PIN Block
ARQC & No CVM or Signature
Remove Card
Print receipt with Signature or display sign on screen
Approved Capture Signature
Network
Sign
Authorization Response
Approve with PIN
Approve with No CVM
Approve with Signature

Fig. 3.1

3.3.2 All CVMs in the Common AID

The second CVM processing logic alternative ("Alternate 2") is based on a common AID on a card reflecting all CVMs that are generally available under the EMVCo specifications based on a particular card's combination of supported networks. Alternate 2 uses standard EMV processing to perform signature debit transactions originating from U.S. terminals under a signature CVM. Under this Alternate, issuers would configure their common AID to reflect all of the available CVMs accessible to the card based on its specific combination of network affiliations and network product configurations enabled for domestic debit transactions. For example, if a card supports two networks where network 'A' supports signature and online PIN and network 'B' supports online PIN, offline PIN and "No CVM", all enabled for domestic transactions, the card's common AID should reflect the union of all of the supported CVMs across all affiliated networks – signature, online PIN, offline PIN and "No CVM". Using this method, a merchant can originate any transaction on a non-PIN CVM as either a signature CVM or "No CVM" transaction.

From a technological perspective, the only difference between Alternate 1 and Alternate 2 is that under Alternate 2 the card can have both the signature CVM and the "No CVM" on the card. The terminal can support either signature CVM or "No CVM" or both. Depending on which was chosen, the host decisioning as to which CVM actually applies to the transaction would still hold.

Figure 3.2 below shows a flowchart describing the processing logic of Alternate 2.

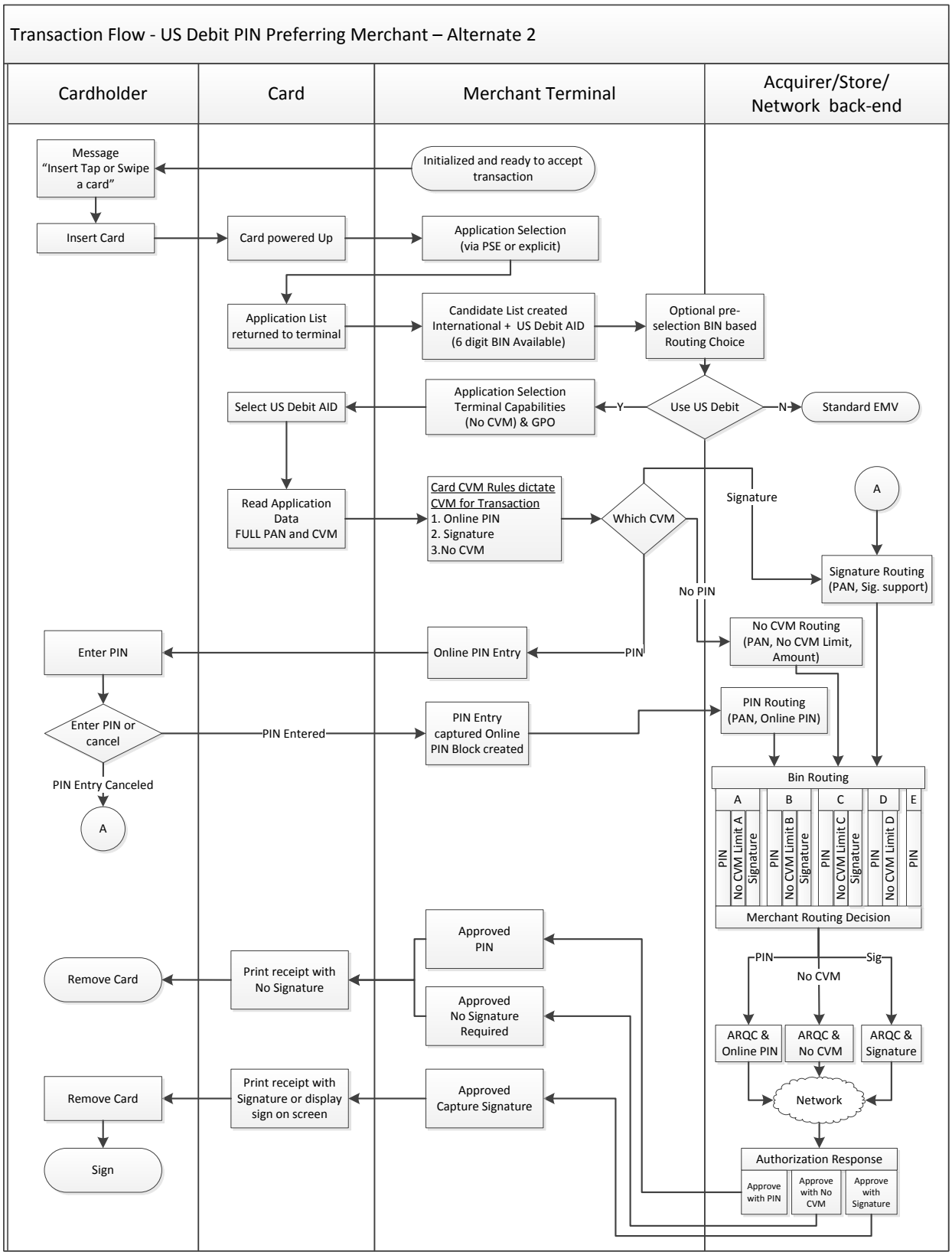

Transaction Flow - US Debit PIN Preferring Merchant – Alternate 2
Cardholder
Card
Merchant Terminal
Acquirer/Store/ Network back-end
Message "Insert Tap or Swipe a card"
Initialized and ready to accept transaction
Insert Card
Card powered Up
Application Selection (via PSE or explicit)
Application List returned to terminal
Candidate List created International + US Debit AID (6 digit BIN Available)
Optional pre-selection BIN based Routing Choice
Select US Debit AID
Application Selection Terminal Capabilities (No CVM) & GPO
Y
Use US Debit
N
Standard EMV
Read Application Data FULL PAN and CVM
Card CVM Rules dictate CVM for Transaction
1. Online PIN
2. Signature
3.No CVM
Which CVM
Signature
A
Signature Routing (PAN, Sig. support)
No PIN
Enter PIN
Online PIN Entry
PIN
No CVM Routing (PAN, No CVM Limit, Amount)
Enter PIN or cancel
PIN Entered
PIN Entry captured Online PIN Block created
PIN Routing (PAN, Online PIN)
PIN Entry Canceled
A
Bin Routing
A
B
C
D
E
PIN
No CVM Limit A
Signature
PIN
No CVM Limit B
Signature
PIN
No CVM Limit C
Signature
PIN
No CVM Limit D
PIN
Merchant Routing Decision
PIN
Sig
No CVM
Approved PIN
Remove Card
Print receipt with No Signature
Approved No Signature Required
ARQC & Online PIN
ARQC & No CVM
ARQC & Signature
Network
Remove Card
Print receipt with Signature or display sign on screen
Approved Capture Signature
Authorization Response
Approve with PIN
Approve with No CVM
Approve with Signature
Sign

Fig. 3.2

3.4 Consumer's Choice Transaction Processing Flow

Merchants may choose to offer a choice to the consumer to use PIN or signature – the so-called "Debit/Credit" button. To enhance the consumer experience, the merchant may choose to deploy a messaging dialogue appropriate to the card inserted. The Solution offers distinct decision-making information without the need to have a BIN table at the POS and to identify the card as U.S. debit issued card. Presence of tag 5F56/42 in the PSE and/or FCI will allow the merchant to either display "Debit/Credit" or "PIN/signature". If the card inserted is not a U.S. issued debit card, the merchant may choose not to display such message and thus offer a better user experience for credit and internationally-issued debit cards.

3.5 Proprietary ATM Card

In context of this section, proprietary ATM cards are ATM cards that are issued by financial institutions and are not payment network branded (e.g., Visa, MasterCard). They are accepted at certain ATM network(s) and may also be accepted at merchant(s) if enabled in debit card point-of sale network(s). The Solution described can be used for deploying proprietary ATM private label debit cards. The issuer may choose any of the three available U.S. common AID Offered Solutions and deploy as described in this document. Should the card require a distinct network identifier for in-network vs. out-of-network processing, this can be achieved in the same manner as branded cards – by adding a network-specific AID which will be personalized on the card, in addition to the common AID. Closed loop cards are outside of the scope of this document.

4 Messaging Implications

In order to support the “No PIN” option in Alternate 1 and Alternate 2 CVM processing and allow the flexibility for the store/acquirer host to decide what the “No PIN” option will be based on the final network that the transaction is routed to, a new field in the message back to the device needs to be added. Since each network will need to decide who will be responsible to populate this field (acquirer, network or issuer), that decision will impact which message specification this field needs to be added to. Further work is required to determine the signature capture requirement under a “No PIN” transaction.

At a minimum it will be required that each acquirer define within its message specification where this indicator will be placed in the authorization response message, the values of this indicator, and the requirements to execute at the device level for each value received (e.g., when to use the indicator instead of the CVM results to decide what the final CVM is).

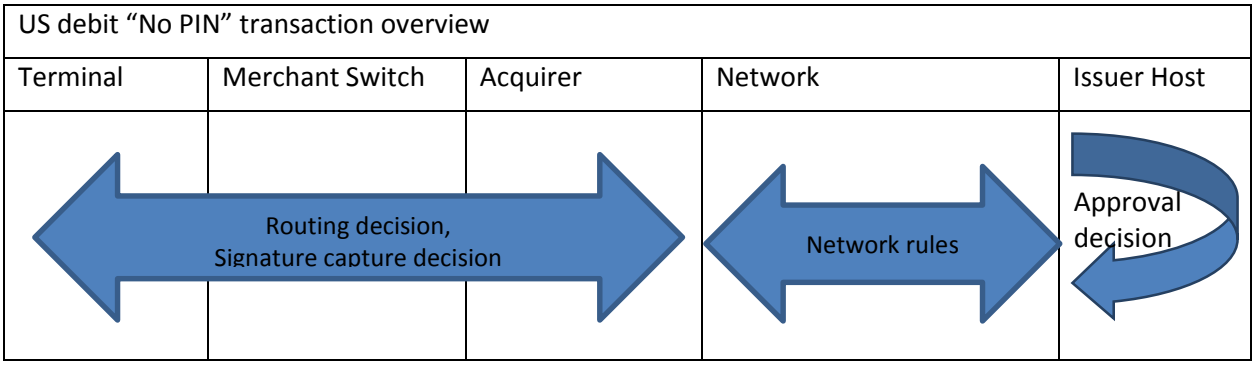
5 Acquirer Routing Guidelines

EMV requires changes to existing acquiring routing processes. It is recommended that acquirers add the "No PIN" indicator as described in Section 4.

5.1 No PIN Transaction Routing and Signature Capture Decision

In a "No PIN" transaction, it is important to identify which entity should make the decision to prompt for signature capture and how.

In a simplified implementation scenario, the merchant store system or merchant's acquirer will be able to determine the outcome at the time it selects its routing path. This paper assumes that the logical place to implement these network rules and issuer preferences is at the merchant's payment system or the acquirer's host.



5.2 Routing Table

In order to make the appropriate routing and signature capture decision, the merchant's payment system or acquirer's host should acquire the following information from the payment networks and possibly issuers. The acquirer will know which networks are EMV-enabled. A BIN routing table example is shown below.

BIN	Network	MCC	Online PIN	No CVM	No CVM limit	Signature support	EMV Supported
444444	A		Y	Y	$50	Y	
			Y	N	$0	N	
	B		Y	Y	$25	N	
	C		Y	N	$0	N	
555555	A		Y	Y	$50	Y	
			Y	N	$0	N	
	B		Y	Y	$25	N	
	C		Y	N	$0	N	
XXXXXX	B		Y	Y	$50	N	
	D		Y	N	$0	N	

6 EMV Acceptance at POS Devices

There are several issues that need to be addressed at the POS device level.

6.1 Selection of the U.S. Common Debit AID

To facilitate routing a debit transaction to multiple networks supported by the card/issuer, the U.S. common debit AID should be selected by the device. Based on the current Offered Solutions proposed by the payment networks, the U.S. common AID may not be the highest priority.

The EMV specifications describe two standard options for application selection:

a. Automatically based on application priority.
b. Consumer selection. Merchant may choose to present the consumer a choice by displaying the application labels as coded by the issuer on the card.

It is recommended that the device should support cardholder selection to allow cardholder choice (see Section 6.4 for further information on multi-application cards). As there will be more than one AID, the application selection process should be done outside the kernel to minimize the impact to certification (unless the kernel supports such logic).

Based on the solution implementation, the device should store a list of all U.S. common AIDs it seeks to accept and once the U.S. common debit AID is identified, the device may select the U.S. common debit AID even though it will not be the highest priority in the card. It is important to note that the selection of the U.S. common debit AID is not mandatory; however, by not selecting the U.S. common debit AID, the merchant may limit their choice of debit routing.

6.1.1 U.S. Territories and Protectorates

In order to allow the various debit solutions to be accepted in U.S. territories and protectorates, there is a need to be able to enable the U.S. common debit AID to be used with cards and/or devices which are set up to have a different country than U.S. (0840). The following two options are available. Please refer to the payment brands and their rules for more details:

a. Option 1 is to enable the U.S. common AID to support international cash, goods, services and cashback (only if supported for domestic as well) in the Application Usage Control (AUC - Tag 9F07 – byte 1 bit 7, byte 1 bit 5, byte 1 bit 3 and byte 2 bit 7). The AUC is used during processing restrictions and is used in conjunction with the Terminal Country Code (Tag 9F1A) and Issuer Country Code (Tag 5F28). If the Terminal Country Code = the Issuer Country Code then it is considered a domestic transaction; if not, then it is considered an international transaction. As the U.S. territories and protectorates may use other Issuer Country Codes and/or Terminal Country Codes (other than 0840) these transactions will be considered international; therefore, if the international bits are not enabled in the AUC, it will trigger a Service not allowed for card product in the TVR (Tag 95 byte 2 bit 5), which in turn may cause the transaction to decline.
b. Option 2 is to set the AUC bits of the U.S. common AID for domestic use only (Tag 9F07 – byte 1 bit 8, byte 1 bit 6, byte 1 bit 4 and byte 2 bit 8). As described in option 1, if the international bits are not set in the AUC and the Terminal Country Code and Issuer Country Code are different, the transaction may be declined. To avoid such a problem, as long as the Terminal Country Code for the U.S.common debit AID (and only this AID) is set to U.S. (Tag 9F1A = 0840)and the Issuer Country Code for the U.S. common debit AID is set to U.S. (Tag 5F28 = 0840), the international

bits can be left set off as this will always be considered a domestic transaction. This will be considered domestic even in cases where the other terminal AID country codes and/or Issuer Country Codes for other AIDs on the card may be set to something else (other than 0840). Cards issued in U.S. Territories (i.e. Puerto Rico) must include the U.S. common AID using an Issuer Country Code (Tag 5F28) = U.S. Defining terminal country is a part of a risk-specific data set associated with a specific RID applicable to the U.S. common AID.

6.2 Terminal Configuration (Terminal Capabilities)

Terminal Capabilities (tag '9F 33') for U.S. common debit AID should be configured as follows:

- To facilitate Alternate 1 CVM processing, the terminal CVM capabilities should include online PIN and "No CVM". Note that future signature support for two or more unaffiliated networks will not impact terminal configurations/CVM capabilities and should be handled outside the kernel as an outcome of a "No CVM" transaction.
- To facilitate Alternate 2 CVM processing, the terminal CVM capabilities should include all CVMs supported under a U.S. common AID which offers Alternate 2 CVM processing. It is an issuer decision which PIN option to support (online/offline)[1]and if "No CVM Required" will be supported. Please refer to Offered Solution specifications for further clarification on Terminal Capabilities configuration for Alternate 2 CVM processing.

6.3 CVM Support

6.3.1 PIN Preferring Merchants

For merchants not using the credit/debit button, the kernel configuration must support PIN cancel to enable the consumers to opt out of PIN. If PIN is entered, the transaction will continue as it does today and the same routing choices will apply. If PIN is canceled, provided this is permitted by the issuer in the CVM list, the merchant will then enter into a "No PIN" CVM option, where the decision of signature or "No CVM" may be sent back in the response from the acquirer. In cases where the new signature indicator is not supported, the merchant should use the EMV CVM Results to decide whether to capture a signature or finalize the transaction with "No CVM".

6.3.2 CVM using the Credit/Debit Button

For merchants using the credit/debit button, this will require support for a Selectable Kernel but not support for PIN cancel. Merchants who decide to support this Selectable Kernel should consult their device manufacturer on how this will be supported.

The consumer choice and IIN (BIN) provided in the FCI prior to the final application selection may drive a Selectable Kernel to use the U.S. common AID or international AID. Alternatively, a merchant offering consumer choice (i.e., cardholder confirmation) should display the Application Label of each AID as a cardholder selection choice. Note, Application Labels are only available after the PSE/FCI of each application has been read. The EMV Terminal Capabilities of the Selectable Kernel are defined at the transaction level.

[1] This option needs to be clarified with merchant acquirer/host provider.

As an alternative to using Selectable Kernel, the merchant has the option to select the International AID when the credit button is selected by the consumer and the Common AID for the debit button.

6.4 Cards Personalized with Multiple Funding Accounts

There may be cases where cards have been configured to support multiple funding accounts (e.g., a card with access to more than one debit account or a card with access to a combination of debit and credit accounts). To properly support such cards, terminal should be capable of supporting cardholder selection as defined in the EMV specifications. Multiple account cards are typically identified by the presence of two or more of the same AIDs which are differentiated through the use of a unique PIX extension. When a terminal determines that multiple accounts exist on a U.S. debit card, the terminal may build a final candidates list containing either each instance of a U.S. common debit AID or each instance of the international brand AID. The terminals must ensure that AIDs not related to a U.S. debit account (e.g., credit) are included in the final candidates list. The remaining AIDs in the candidates list should then be presented to the cardholder to allow for their final selection. Issuers should ensure that meaningful descriptors are used in the Application Labels and Application Preferred Names of each AID to help guide the cardholder through the selection process and avoid potential cardholder confusion.

For a credit or debit card that does not support U.S. common debit AID, having only international or proprietary AIDs, the terminal should prepare an application selection for the consumer of the AIDs following EMV standards of handling PIX extension.

Based on the consumer selection, the transaction will continue in its standard course based on the CVM settings and outcome as described in this document.

7 Conclusion

The proposed Solution presents two CVM processing options to satisfy all merchant and issuer requirements listed in Section 2.

Industry stakeholders will need to independently decide what approach best suits their own respective preferences and business needs, and implement accordingly. Decisions in this regard are likely to reflect availability of corresponding solutions in the market and the terms of the business agreements negotiated with other relevant contract parties. The EMV Migration Forum does not and cannot take a position on either approach.

The Solution does not require any new (non-EMV) data elements, thus minimizing or eliminating the need for new EMV or brand type approvals.

The technological principles described in this paper allow issuers to deploy Reg II compliant and future-proofed EMV debit cards with presently available card products.

The Solution offers merchants a technological path to develop and deploy multi-network routing debit EMV solutions with the assurance that hardware and software choices will satisfy present and currently foreseeable future regulatory requirements.

As previously noted, however, the Solution is high-level. Accordingly, stakeholders interested in implementing an actual solution consistent with the proposal will need to develop their own detailed specifications, and should consult with appropriate issuer, acquirer and payment network partners prior to any debit implementations.

8 ADDENDUM I – U.S. Common Debit Contactless Acceptance

Note: This addendum was published in May 2015.

8.1 Fundamentals – Contactless Acceptance

The U.S. Debit EMV Technical Proposal is compatible with a contactless transaction when implemented on a dual interface EMV chip card or a mobile device.

This addendum describes a method for achieving successful contactless multi-network transaction processing while preserving global interoperability using a U.S. Common Debit compliant EMV application configuration.

8.2 U.S. EMV Common Debit Compliant Issuance

Financial institutions considering issuance of mobile payment credentials or dual Interface EMV debit cards have the option to deploy a U.S. Common Debit compliant EMV application configuration. There is no need to implement any proprietary functionality. An EMV contactless transaction is always initiated utilizing the PPSE (Proximity Payment System Environment). The POS device will have the ability to identify the account as U.S. debit by reading data from the PPSE as per the U.S. Common Debit payment brand specifications. The PPSE will list both the U.S. Common Debit AID as well as the payment brand global AID. Appropriate data elements – U.S. country code and IIN (6-digit BIN) – will be made available in the PPSE. Application priority of the Common AID vs. the global AID does not influence the selection of one or the other AID. It is the merchant's decision to use either.

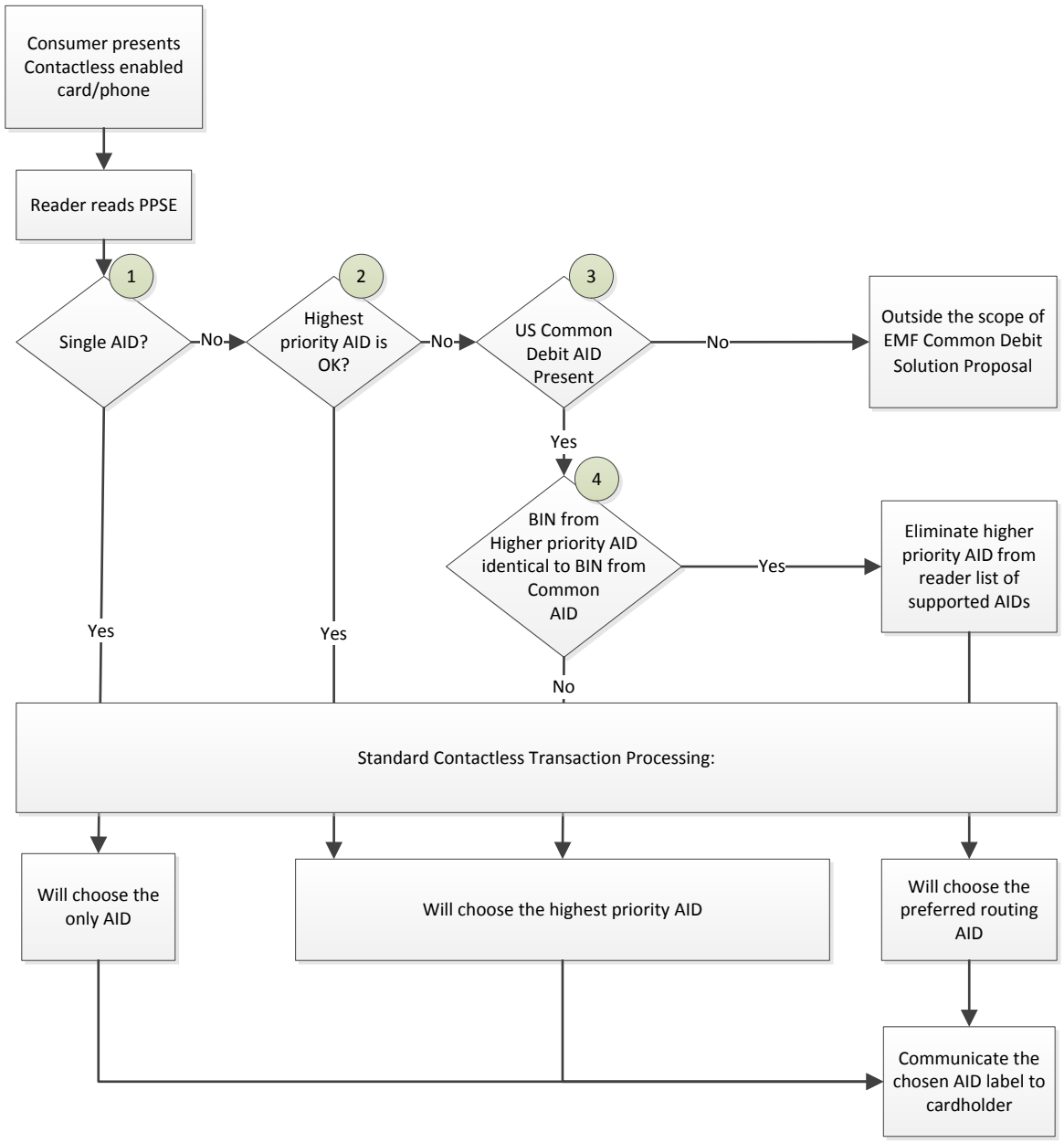
For further details on configuring a dual interface U.S. debit card or mobile payment credential, please seek guidance from the payment networks offering U.S. Common Debit solutions.

8.3 CVM Processing

Online PIN, Signature and No CVM may be supported as per the payment networks' specifications. A No PIN transaction signature capture decision can be implemented the same as with the contact interface – see Sectio 5.1 of the U.S. Debit EMV Technical Proposal.

8.4 U.S. Common Debit AID Selection

The following chart illustrates an example flow for the merchant making a decision to select the U.S. Common Debit AID.



Addendum I – Fig 1 - Common Debit AID selection

Following is an explanation of the decision points as numbered in the flow chart.

1. Should there be a single AID in the application selection candidate list, the terminal will execute a standard contactless EMV transaction, typically the case for credit or international contactless enabled EMV chip cards.
2. If the PPSE contains multiple AIDs but the highest priority AID is a global AID or is otherwise acceptable to the merchant, the transaction proceeds as normal.
3. The presence of the U.S. Common Debit AID which is of merchant's preference and is not the highest priority in the PPSE will initiate U.S. Common Debit specific terminal processing.

4. To ensure that the highest priority AID is of the same funding debit account linked to the common AID, the terminal will compare the BIN (IIN-Tag 42 made available in the PPSE). Should there be no match (for example, a credit/debit or multi-funding account), the terminal will select the highest priority AID. Should there be a match, the terminal will eliminate the higher priority AID from the terminal's list of supported AIDs.