DEBIT NETWORK ALLIANCE

U.S. EMV™ Debit Implementation Guidelines for POS Acquirers

Version 1.0
August 15, 2014

About Debit Network Alliance

Debit Network Alliance LLC (DNA) is a Delaware limited liability company owned by ten U.S. Debit Networks, and open to all U.S. Debit Networks, founded in December 2013. The goal of this collaborative effort is to provide interoperable adoption of chip technology for debit payments, while supporting security, innovation, and optimal technology choice. Further, the company has worked to bring about perpetual access to the technology deployed to accomplish EMV™ in the US, and support for all transactions types (PIN, signature, "No CVM") supported by the debit networks both existing and future.

The debit networks have a long history of working collaboratively - especially with regard to improving security - to define standards that maintain the integrity and quality of the U.S. payment industry.

The founding networks of Debit Network Alliance are AFFN®, ATH®, CO-OP Financial Services®, Jeanie®, NETS®, NYCE®, Presto!®, PULSE®, SHAZAM®, and STAR®.

EMV™ is a trademark owned by EMVCo LLC.

This document does not necessarily express the views and opinions of every member of DNA. Companies should consult their own legal counsel or other competent advisors for definitive advice on how to address the matters identified in this document.

TABLE OF CONTENTS

1 Introduction

1.1 Executive Overview

As a result of the publicity surrounding recent data breaches, and the rise of counterfeit card fraud, there are few people in the U.S. payments industry who are unaware of chip cards and EMV. However, the details of EMV, and how to implement it, remain a mystery to many.

Although the global card brands have announced roadmaps with liability shift incentives, deployment of EMV for debit has been slow due to the complexity inherent in debit in the U.S. With debit, there are multiple U.S. debit networks on a card as well as legislation (e.g., Regulation II) specifically for debit. These requirements and recent court rulings uphold merchant routing choice and highlight the need to "future proof" functionality in case of further regulatory action. (On the other hand, FI-issued credit card EMV implementation is much simpler because of the single brand nature of these products.)

Furthermore, issuers want to maintain their ability to easily switch networks for business reasons without reissuing cards; while, merchants (and acquirers) want to maintain their ability to choose the network for debit routing.

Financial institutions need debit. It helps them serve their customers more efficiently and cost-effectively.

Customers demand debit. Debit cards are a favorite form of payment instrument among consumers.

The cost of payments is one of a merchant's largest expenses. Maintaining a competitive environment is one of the best ways that the merchant community can maintain control of their payment environment and routing options, and keep payment costs from escalating out of control. Merchants can ensure this competitive environment by retaining the ability to route to multiple debit networks when implementing EMV within the POS terminal and host routing logic.

This document describes the challenges that global payment network requirements and U.S. legislation present for the U.S. debit networks and the U.S. EMV migration, and the solution to these challenges. This document outlines the best practices related to the implementation of EMV for domestic debit Point of Sale (POS) transactions when a global brand is one of the brands on the card and the Debit Network Alliance's requirements when a global brand is not present on the card.

Although this document focuses on POS, the DNA recognizes the critical role that ATMs play in our industry. Please refer to the DNA's web site for ATM-related reference material, including a recorded webinar about EMV for ATM Owners and Deployers, and an ATM best practices document.

A glossary at the end of this document contains descriptions of terms which may be unfamiliar to the reader.

For those interested in more technical details, Appendix A includes a brief history of EMV and EMVCo, and explains some basic EMV concepts and terminology.

The following symbols are used throughout the document:

	**Indicates a DNA requirement.**
	Indicates a DNA recommendation or best practice.
	Indicates a definition required for readability of this document.

In addition to reviewing this document, merchants and acquirers must obtain the current specifications from all networks or destination points to make sure it is clear what EMV data elements are supported by each specification, and where it must be placed within the messages exchanged between the terminal and the acquirer.

For additional information, please contact your debit network representative.

1.2 Document Version History

Version Number	Date	Changes
1.0	August 14, 2014	Initial Publication

1.3 Purpose

The purpose of this document is to focus on requirements for implementing the global brands' Common AIDs and DNA's Shared Debit AID. Within this document, the term "global AID" will mean the AID present on the card that is utilized by the global (international) brand whose logo is on the card. The global brands are American Express, Discover, MasterCard, and Visa. Global AIDs include those owned by American Express, Discover, MasterCard Debit/Credit, MasterCard Cirrus, MasterCard Maestro, Visa PLUS, Visa Electron, etc. The term "DNA Shared Debit AID" will refer to the debit AID offered by the DNA for use on debit or prepaid cards that do not carry a global brand's AID. The Debit Network Alliance has used the adjective "Shared" instead of "Common" to reflect the shared and interoperable governance structure as promoted by the DNA. This document refers to all four debit AIDs as "U.S. Domestic Debit AIDs" or "USDDAs."

2 U.S. Debit: An Evolving Landscape

2.1 A Brief History of U.S. Debit Networks

American financial institutions initially developed debit cards for use at ATMs as a way to reduce costs associated with check processing and live tellers. ATM networks were formed to allow wider access to services such as cash withdrawals, and in fact were mandated by law in several U.S. states. These networks soon became the standard for banks and credit unions offering ATM services.

After a number of years, the ATM networks took the logical step of extending debit to Point of Sale (POS). Little or no interchange fees were charged, and some networks did not collect any fees from the merchants who accepted debit cards.

Historically, debit networks were divided between signature networks and PIN debit networks. Because PIN pads were not commonly used by many merchants, PIN debit volume grew slowly. However, as a result of the reduced costs for issuers, enhanced security and convenience for cardholders and merchants, by the early 1990s debit had reached critical mass in the U.S.

The major global (signature-based) payment networks responded with new versions of their debit products. They initially formed partnerships with the existing PIN debit networks, leveraging their technical infrastructure to provide connectivity to the card issuing FIs. Over time, the global signature networks built a huge presence in the debit market, largely through incentive pricing.

Initially, a significant number of issuers chose their network participation based on signature vs. PIN. In recent years, the global networks have created operating rules requiring issuers to accept all cardholder verification methods (PIN, signature, and none) for magnetic stripe debit cards. These new operating rules have created significant controversy among issuers as well as merchants. By providing incentives to the merchant community, the global payment networks have increased their routing share for all transaction types.

Most U.S. debit networks are licensing the MasterCard, Visa, and Discover chip applications and Common U.S. Debit AIDs[1] in order to support EMV in the U.S. These licensing agreements enable debit networks to provide issuers with portability and merchants with routing choice, but they also may limit the debit networks' ability to introduce new innovation – even innovation that will produce more advanced security.

[1] A detailed definition of the term "AID" may be found in Appendix A.3.

2.2 Preserving Routing Choice When Implementing EMV

As most payment companies are aware, implementing EMV and chip card acceptance at the POS will require extensive hardware and software changes. During the past twenty four months, the debit industry has wrestled with a solution for how to provide routing choice for merchants and issuer portability (the ability to easily re-brand debit cards when adding or switching networks). After much hard work, the industry agreed to support Common U.S. Debit AIDs. Common U.S. Debit AIDs are AIDs ***licensed by their owners on a bilateral basis*** to other networks for limited usage purposes. To date, there are three Common U.S. Debit AIDs, one each by VISA, MasterCard and Discover. In addition, the Debit Network Alliance has developed a debit AID that is owned by all DNA members and is ***licensed by the DNA to other networks in a shared governance manner***…thus the DNA Shared Debit AID moniker. This DNA Shared Debit AID will be used on cards that do not have one of the global brand AIDs present but has at least two unaffiliated debit brands on the card. Functionally, the Common U.S. Debit AIDs and the DNA Shared Debit AID are equivalent. The main difference is in the multi-lateral, shared governance nature of the license and business terms. For ease of reading, throughout the rest of this document we will refer to all four such AIDS as "U.S. Domestic Debit AIDs" or "USDDAs." Unless each merchant and acquirer understands how to design their POS system to choose U.S. Domestic Debit AIDs included on debit and prepaid debit chip cards, they may lose their ability to control debit routing and, therefore, the associated economic benefits.

USDDA → Throughout the rest of this document, the acronym USDDA (U.S. Domestic Debit AID) refers to any of the AIDs that allow multi routing capabilities through BIN routing. These would include the following AIDs (as of this writing):

- DNA Shared Debit AID
- Discover US Common Debit AID
- Maestro US Common Debit AID
- Visa US Common Debit AID

Regulation II (the Durbin Amendment)-compliant debit and prepaid debit chip cards will likely have one global AID plus either a Common U.S. Debit AID or the DNA Shared Debit AID. **The AID that is selected at the POS plays a critical role when determining transaction routing.**

As long as all U.S. POS devices always choose a U.S. Domestic Debit AID when one of these AIDs is present on a debit or prepaid debit chip card, all organizations can continue to use the same BIN table routing used in today's magnetic stripe environment, thus controlling routing choice.

The DNA is pleased to announce that we have registered our DNA Shared Debit AID with the International Standards Organization. ISO has assigned A0000006200620 as the AID value. This is an important milestone toward enabling participants to issue Regulation II-compliant chip cards with multiple regional DNA networks branded on the card. DNA-supported applications must comply with the EMV Common Core Definition (CCD) specification.

POS acquiring processors and merchants need to recognize all published USDDAs to continue to maintain routing choice. As previously noted, each debit and prepaid debit card will have only one USDDA.

This white paper includes requirements and best practices for merchants and POS acquiring processors to support USDDAs. These requirements and best practices are described in more detail in the following sections of this document.

3 The U.S. Debit EMV Solution

A chip card may contain multiple AIDs. When there is only one AID on a card, and it is a global AID, the global payment networks require that transactions initiated by that card must be routed to the owner of that AID. For example, when a global MasterCard AID is selected when initiating a transaction, the transaction must be sent to MasterCard, just as when a global Visa AID is selected when initiating a transaction, the transaction must be sent to Visa.

As a result of the prioritization of the global AIDs in the chip, the way the EMV specifications define Application Selection, and the global payment network requirements, the issuer (or even the cardholder) may determine how a chip transaction is to be routed, based on the AID that is selected for that transaction.

Regulation II allows U.S. merchants to make the network routing decision for debit cards. If there are multiple AIDs on the card, the terminal must be able to select an AID that will preserve merchant (acquirer) routing choice. This may not be the AID that would normally be selected using the standard EMV Application Selection logic described in the EMV specifications.[2]

3.1 The Impact of EMV to the U.S. EMV Migration

The global payment network requirement cited above posed two challenges to the U.S. EMV migration:

- It does not comply with Regulation II regarding POS routing choice
- The Federal Reserve Board "has prohibited issuers and networks from limiting available routing options for debit card transactions to fewer than two unaffiliated networks per debit card. Accordingly, all debit cards will need to participate in at least two unaffiliated networks so that transactions initiated using those debit cards will have at least two independent routing channels. The two unaffiliated networks could be one PIN network and one signature network (the most common configuration), two signature networks, or two PIN networks (in each case as long as the two networks are not affiliated)."[3]

As a result, if U.S.-issued debit chip cards only supported the global AIDs currently provided by Discover, MasterCard, and Visa, all transactions performed by a U.S.-issued debit chip card at a U.S. chip-enabled terminal would be routed to the global payment network owning the global AID used for the transaction. Clearly, this was unacceptable to the U.S. debit networks and for Regulation II compliance.

In addition, some financial institutions issue debit cards that do not carry a global brand. An AID was needed for these cards so that the debit networks present on the card could allow for merchant routing choice in compliance with Regulation II. The DNA Shared Debit AID fulfills this need.

[2] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3, November 2011, Book 1, Section 12
[3] Alston Bird Financial Services and Products Advisory, June 30, 2011 "Federal Reserve Board Issues Final Rule to Implement Durbin Amendment"

3.2 Key Aspects of the U.S. Debit EMV Technical Proposal

An EMV Migration Forum debit working group diligently gathered facts and consensus-based preferences from participating industry stakeholder groups in order to devise a technological path for implementing EMV debit in the U.S. while working within existing legislation and accommodating foreseeable future routing requirements set by the industry and/or regulators.[4] Key characteristics of the solution include:

- Allows the merchant's terminal to select a U.S. Domestic Debit AID (USDDA) when accepting a transaction, which facilitates multi-network debit transaction routing.
- Requires no changes to the terminal's EMV kernel.
- Supports any form of cardholder verification, card authentication, or transaction authorization described in the EMV specifications.
- Provides flexibility at the terminal for cardholder verification method (CVM). Refer to Appendix A.8 for more information about CVMs.

The use of a USDDA, and options for CVMs, are discussed below. Please refer to the EMV Migration Forum Debit Technical Working Group's U.S. Debit EMV Technical Proposal[5] for additional details.

3.3 U.S. Domestic Debit AIDs

A Common U.S. Debit AID is one that is owned by a global card brand, but can be licensed by a debit network. Discover, MasterCard, and Visa will each license a Common U.S. Debit AID.[6] The DNA will license a Shared Debit AID to debit networks for cards that do not have a global brand. Any debit network licensed on one of the USDDAs is available through that AID.

In order to allow routing choice within the U.S., a U.S.-issued debit chip card must contain one (but only one) of the USDDAs.[7] A U.S.-issued debit chip card that has a global brand may also contain one or more global AIDs associated with that global brand. This allows the card to be used at chip-enabled terminals outside of the U.S., since those terminals may not support a USDDA.

U.S.-issued debit chip cards that are branded as Discover, MasterCard, or Visa will contain the Common U.S. Debit AID associated with that brand, and may also contain one or more global AIDs associated with that brand. For example, a U.S.-issued MasterCard debit chip card will contain the MasterCard (Maestro) Common U.S. Debit AID, and may also contain one or more global MasterCard AIDs (e.g., MasterCard Debit, MasterCard Cirrus).

---

[4] EMV Migration Forum Debit Technical Working Group U.S. Debit EMV Technical Proposal, Version 1.2, April 2014.
[5] Ibid.
[6] American Express is not licensing a Common U.S. debit AID. American Express is a closed-loop payment system. When an American Express credit card is accepted, the resulting transaction is routed to American Express. This current practice will not change with the introduction of EMV.
[7] EMV Migration Forum Debit Technical Working Group U.S. Debit EMV Technical Proposal, Version 1.2, April 2014.

U.S.-issued debit chip cards that are branded without a global brand will contain the DNA Shared Debit AID associated with the debit networks that joined DNA and licensed the AID. For example, a U.S.-issued debit chip card with the STAR and NYCE networks will contain the DNA Shared AID. Refer to Section 7 for more information about how an issuer's implementation of EMV can impact merchants.

U.S. chip-enabled terminals must support global AIDs, plus all of the USDDAs for the networks in which they participate. In order to ensure routing choice, a U.S. chip-enabled terminal must be able to select a USDDA over a global AID, when the chip card and the terminal support both. (Global brands will also be part of their licensed Common AIDs.) Refer to Sections 5 and 6 for more details about impacts to merchants and acquirers.

Through the proper use of the USDDAs, debit network priority routing rules for merchant routing choice can be preserved.

3.4 Options for Cardholder Verification

The EMV specifications allow online PIN, signature, and "No CVM Required" (often referred to as "No CVM") as cardholder verification methods[8]. All three are supported by the U.S. Debit EMV Technical Proposal. Note that offline PIN is outside the scope of the proposal and will not be addressed in this document.

3.4.1 Online PIN

Online PIN is widely used in debit transactions today. Many issuers support more than one PIN debit network. Support for online PIN functionality with a chip card is no different than the way online PIN is supported today with magnetic stripe cards.

Because online PIN is already familiar to U.S. debit cardholders, and there is already an infrastructure to support it in the U.S., online PIN will be used as the primary CVM for USDDAs. However, merchants may also need to support additional CVMs, as described below.

3.4.2 "No CVM"

In EMV terminology, "No CVM" is an option whereby the consumer does not enter a PIN or a signature at the POS. "No CVM" is an important option for low value transactions performed by debit cards. A merchant can establish a threshold (floor limit) under which neither PIN nor signature is required.

There are two ways that a merchant can support transactions using "No CVM":

PIN preferring merchants: a PIN entry message will always be presented to the consumer regardless of the amount of the transaction. If the consumer opts out of PIN, the merchant will initiate a "No CVM" ("PINless") transaction. The amount of the transaction, plus 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

[8] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3, November 2011, Book 3, Section 10.5

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: Merchants whose primary goal is to achieve fast customer service may choose to use "No CVM" as a primary CVM by establishing a lowest common "No CVM" limit value over all the supported networks. When the transaction amount is below this limit, the merchant will skip PIN entry and use the "No CVM" option directly. If the amount is above the lowest common "No CVM" limit, the merchant has 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 complete as "No CVM" over a network that supports a higher limit or a network that will have indicated that a signature is required.

3.4.3 Signature

For the USDDAs, signature transactions can be facilitated via the "No CVM" option on the card. Please refer to section 3.5 for more information.

3.5 Future-Proofing Debit EMV with a USDDA

Although the goal of the EMV Debit Technical Working Group was to achieve a consensus using a single solution for support of signature transactions, two alternate conceptual solution frameworks emerged for CVM processing logic. Either of these two CVM processing approaches provides both merchants and issuers with a "future proof" solution to implement host-managed CVM processing. Neither alternative forces the use of either single or dual message processing; however, merchants should work with their acquirer/processor when implementing these routing options.

3.5.1 Alternative 1: USDDA with PIN, Signature (via No CVM flag) and No CVM

Alternative 1 proposed in the US Debit EMV Technical Proposal describes how a merchant acquirer can route any transaction, be it PIN, Signature, or small ticket (No CVM) by selecting only one AID on the card, namely the USDDA on the card. If the merchant would like to prompt for PIN, the merchant would then do so and standard BIN routing would take place through any of the PIN networks available on that transaction.

If the merchant acquirer chooses to not prompt for PIN, then the No CVM option is chosen. Based on the network rules, the merchant acquirer can choose to send that transaction as a PINless small ticket transaction (if it's below a certain dollar amount) or the merchant acquirer can choose to send the transaction to a signature capable route and have the customer sign for the transaction. Regardless of the choice, the merchant was able to facilitate these choices by selection one, and only one, AID.

The diagram below presents further details on how the processing will work using Alternative 1.

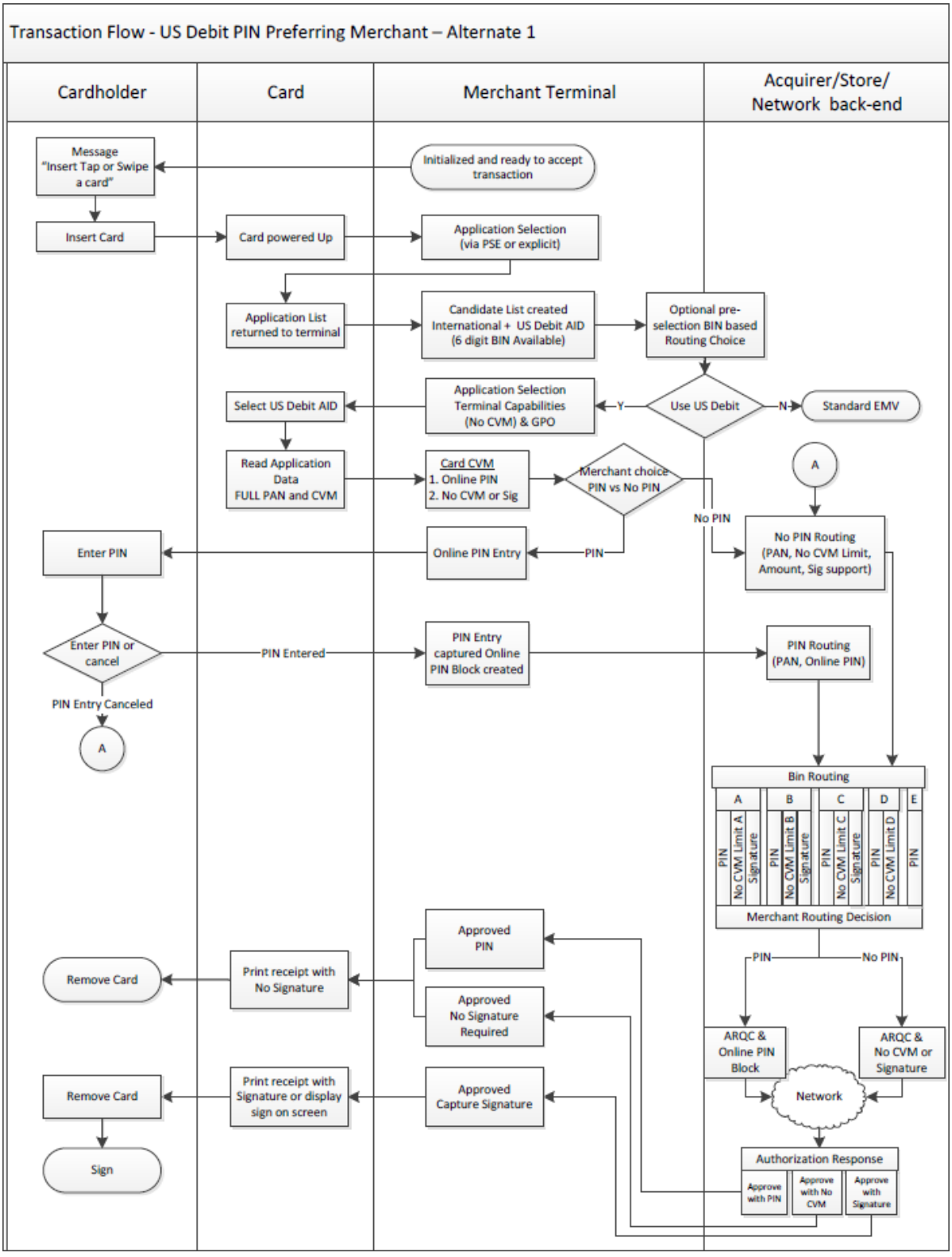

Figure 3-1: CVM Alternative 1

For further information, please refer to the U.S. Debit EMV Technical Proposal, Section 3.3.1.

3.5.2 Alternative 2: Common AID Recognizes All CVMs

This alternative was developed to satisfy the needs of issuers and networks desiring to use all three distinct CVMs (Online PIN, Signature, and "No CVM"). As of July 2014, this alternative is not supported by any USDDA. Refer to Appendix B for more information about Alternative 2.

3.6 The DNA Shared Debit AID

The DNA Shared Debit AID will be used for U.S.-issued debit chip cards that do not have a global brand. These chip cards will contain the DNA Shared Debit AID and only the DNA Shared Debit AID. The use of the DNA Shared Debit AID allows transactions initiated by these debit chip cards to be routed according to existing routing rules.

The DNA Shared Debit AID can represent any EMVCo Common Core Definition (CCD/CPA) compliant chip application.

The DNA Shared Debit AID:

- **Can be used only with a contact EMV application**
- **Supports online authorization**
- **Supports online authentication**
- **Supports online PIN, Signature (via No CVM flag) and No CVM**

The functions that will be supported by the DNA Shared Debit AID are described in more detail below.

3.6.1.1 Chip Card Technology

A debit chip card containing the DNA Shared Debit AID will be a hybrid card, that is, a contact chip card with a magnetic stripe. The DNA Shared Debit AID profile supports contact functionality at this time.

3.6.1.2 Authorization

The DNA Shared Debit AID supports online authorization. It may support offline authorization in the future.

3.6.1.3 Authentication

The DNA Shared Debit AID supports online authentication. It may support offline authentication in the future.

3.6.2 Cardholder Verification Methods

The DNA Shared Debit AID supports multiple Cardholder Verification Methods, including online PIN, signature (via No CVM flag) and "No CVM." However, in order to comply with Regulation II, merchants must have a choice of at least two networks when routing debit transactions. Some networks support PIN, and others do not.

The DNA Shared Debit AID supports online PIN, signature (via No CVM flag) and "No CVM" as described under Alternative 1 (see Section 3.5.1). The DNA Shared Debit AID does not support offline functions at this time. Please refer to Section 3.5 for information on how signature or "No CVM" is determined.

3.6.2.1 PIN

Online PIN is the primary CVM used in single message (SMS) debit transactions today. Many issuers support more than one PIN debit network. Support for online PIN functionality on a chip card is no different than support for online PIN with a magnetic stripe card:

- The PIN Offset (or other data used to verify the PIN, such as the PVV) can be stored on the host system or in the Track 2 magnetic stripe and/or chip data on the card; however, if PIN Change at the ATM is supported, the PIN Offset must be on the host
- The PIN entered by the cardholder is encrypted by the PIN pad at the terminal
- The encrypted PIN is sent online to the host for verification as part of the transaction request message

The DNA Shared Debit AID supports online PIN verification but not offline PIN verification.

3.6.2.2 Signature (via No CVM flag) and "No CVM"

The DNA Shared Debit AID will support signature (via No CVM flag) and "No CVM" transactions as described as Alternative 1. Please refer to Section 3.5.1 for information on how "No CVM" (i.e. signature or "No CVM") is determined.

4 Sample Transaction Scenarios

Several scenarios are presented below, which represent the combinations of card, terminal, and AID(s) that are likely to be seen in the U.S. over the next few years.

4.1 Magnetic Stripe Debit Card at Magnetic Stripe POS Terminal

Magnetic stripe cards and magnetic stripe terminals will be prevalent in the U.S. for several years. Once a merchant, acquirer, or issuer has made changes to their online transaction processing systems or batch systems to support EMV, they should perform regression testing to ensure that magnetic stripe transactions continue to proceed "business as usual." The cardholder swipes the magnetic stripe card at the POS terminal, and magnetic stripe data is used to generate the transaction request message, which is sent online to the host for authorization.

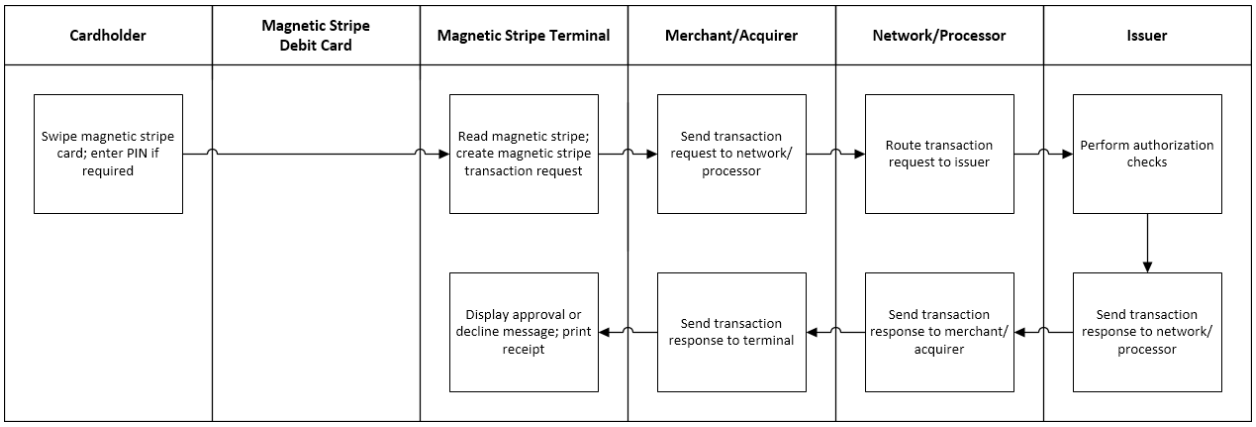

Figure 4-1

4.2 Magnetic Stripe Debit Card at Chip-Enabled POS Terminal

A chip-enabled terminal must continue to support transactions initiated by magnetic stripe cards. The cardholder will swipe the card and the transaction should proceed "business as usual."

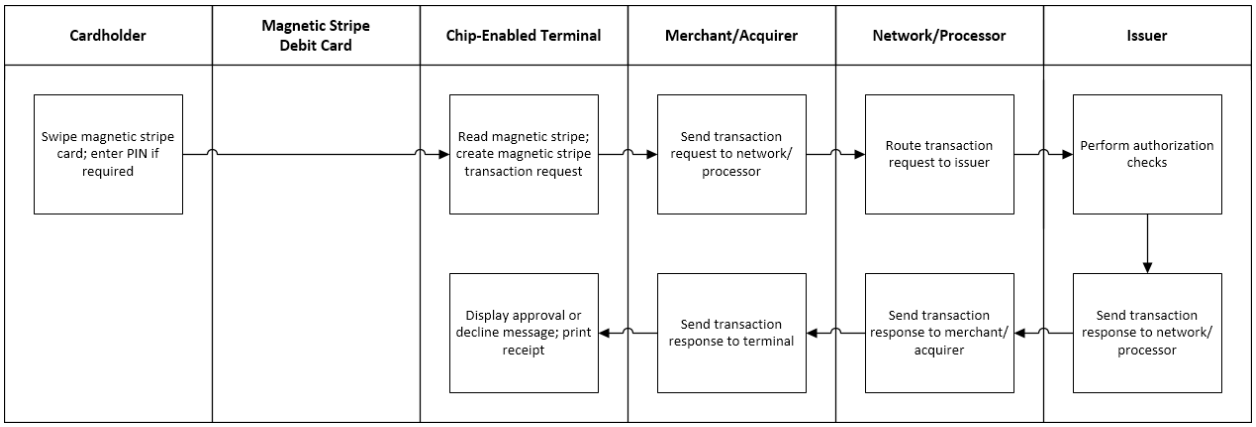

Figure 4-2

4.3 Chip Debit Card at Magnetic Stripe POS Terminal

For a period of time, terminals that only support magnetic stripe technology will still be in use. Some of these terminals may have no place for the customer to insert a chip card. When a chip card is used, the cardholder will swipe the magnetic stripe on the chip card; the transaction should proceed "business as usual."

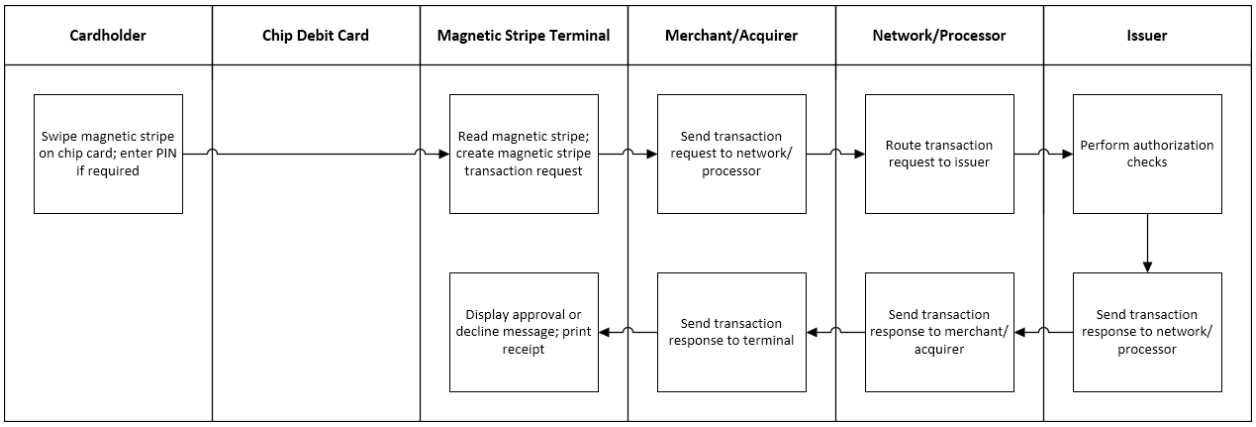

Figure 4-3

4.4 Chip Debit Card at Chip-Capable Terminal; EMV Not Yet Enabled

In some cases, a terminal may have the hardware that is required to support EMV, but EMV has not yet been enabled. This could be because the software or configuration has not yet been loaded into the terminal. When a chip card is presented, the cardholder may see that the terminal has a slot for the chip card, and insert the chip card. In this case, the terminal must prompt the customer to swipe the card. When the cardholder swipes the card, the transaction should proceed "business as usual."

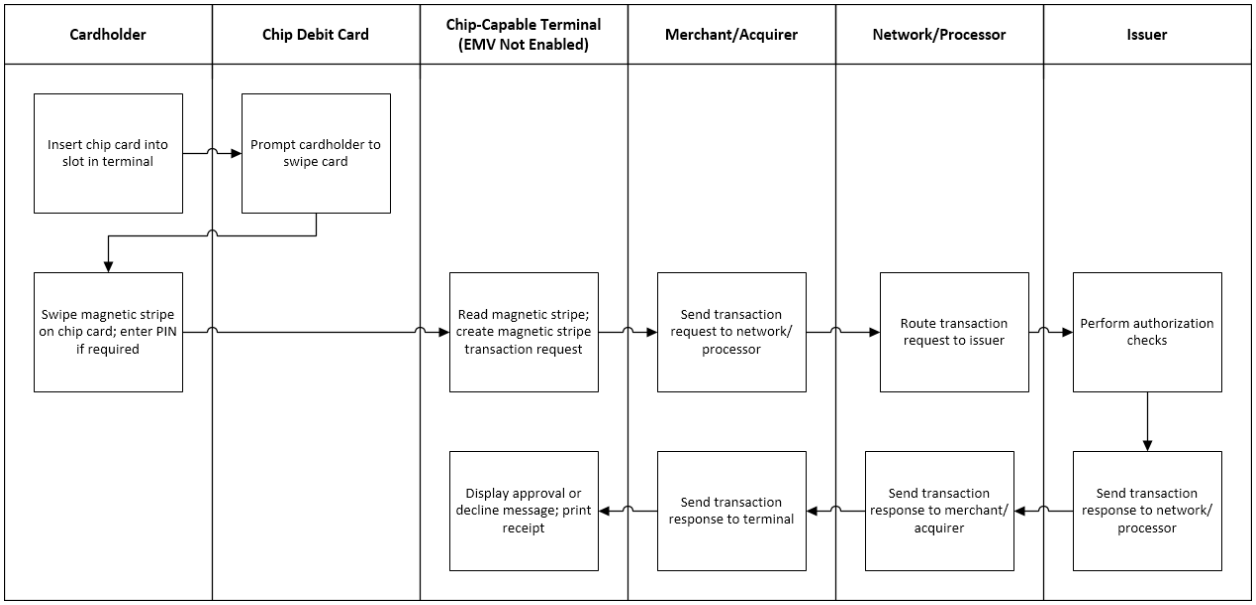

Figure 4-4

4.5 Chip Debit Card at Chip-Enabled POS Terminal; Chip Not Read

This is a "technical fallback," or "fallback," scenario. If the cardholder swipes the card, the terminal should detect that a chip card has been presented, and prompt the cardholder to insert the card. However, when the cardholder inserts the card, if the terminal cannot communicate with the chip (because the chip has been damaged, the terminal card reader is damaged, or other reason), the terminal should prompt the cardholder to swipe the card again. When the magnetic stripe is read, the transaction should proceed "business as usual." Data in the request message (e.g., service code, Track 2 data, and POS Entry Mode) will indicate that this is a fallback transaction. Each issuer will determine the appropriate authorization action to take based on their network regulations, fraud score, risk tolerance, cardholder history, and other factors.

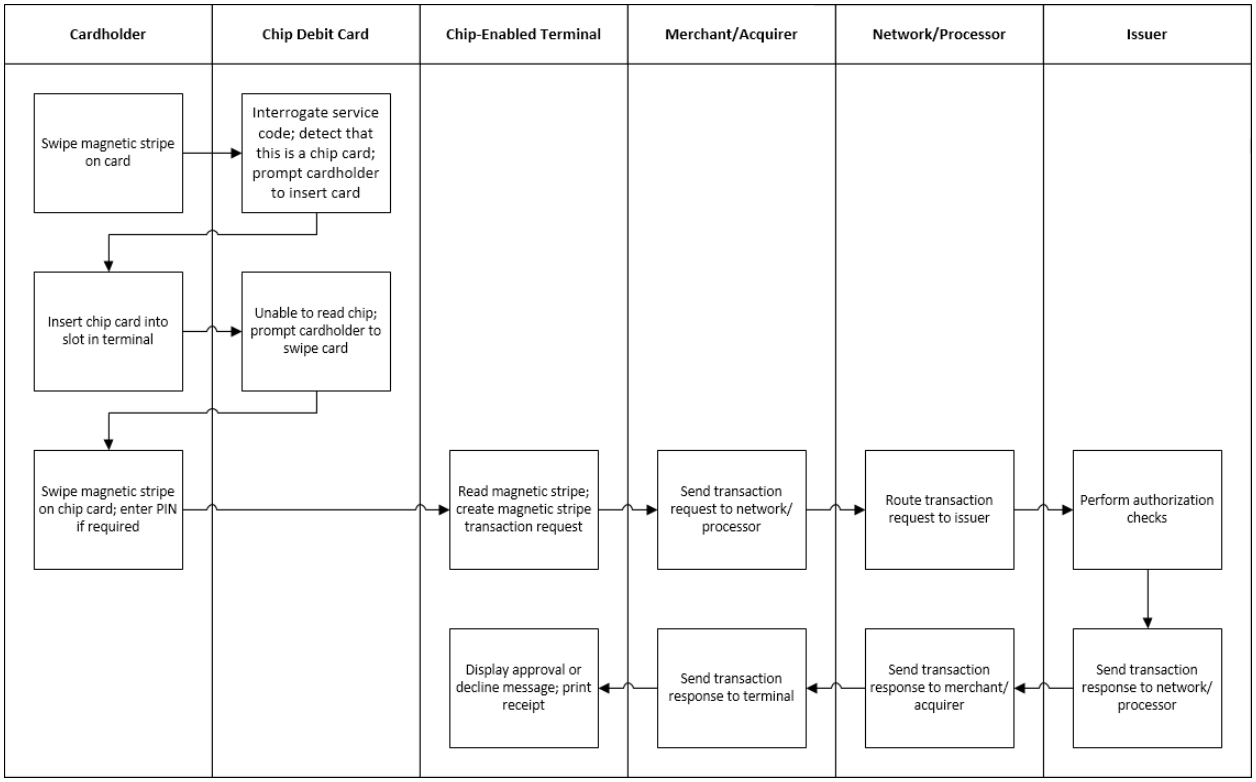

Figure 4-5

4.6 Chip Debit Card with Global AID(s) and No Common U.S. Debit AID (International Issued Card)

If the cardholder swipes the card, the terminal should detect that a chip card has been presented, and prompt the cardholder to insert the card. When the cardholder inserts the card, the terminal will communicate with the chip, and use standard EMV processing to select a global AID and CVM that both the card and the terminal support. The transaction must be routed to the payment network that owns that global AID. For example, if a global Visa AID is selected, the transaction must be routed to Visa.

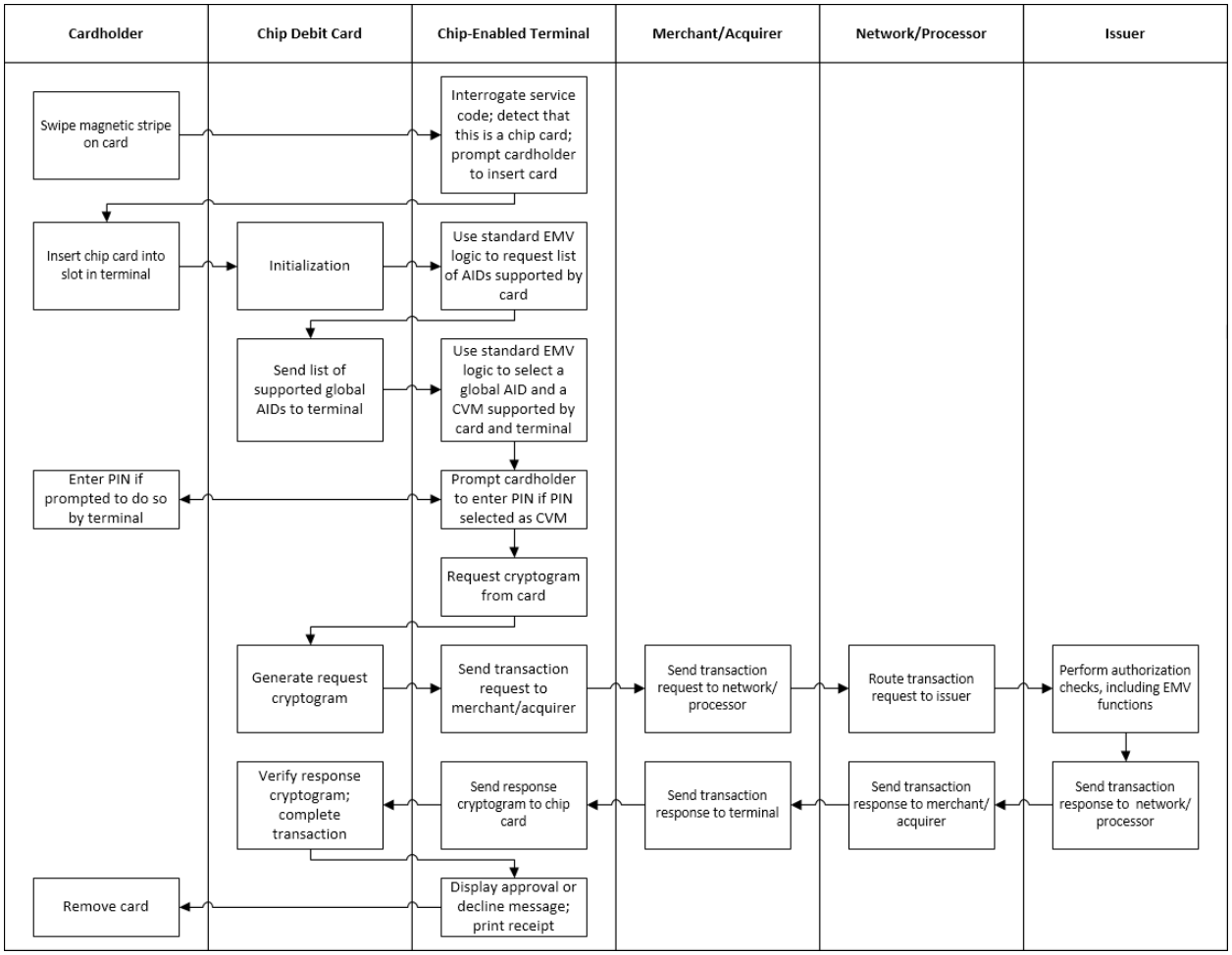

Figure 4-6

4.7 Chip Debit Card with Global AID(s) and a Common U.S. Debit AID

In this scenario a chip debit card containing one or more global AIDs, plus a Common U.S. Debit AID, is presented to a U.S. chip-enabled terminal. The terminal must support the Common U.S. Debit AID(s) for all networks in which the merchant participates. A Common U.S. Debit AID is an AID licensed by Discover, MasterCard or Visa. This scenario does not apply when the DNA Shared Debit AID is on the chip card (that scenario is described in Section 4.8).

If the cardholder swipes the card, the terminal should detect that a chip card has been presented, and prompt the cardholder to insert the card. When the cardholder inserts the card, the terminal will interrogate the chip to see if the chip supports one of the Common U.S. Debit AIDs. Because a Common U.S. Debit AID is present in the chip, the terminal should select the Common U.S. Debit AID over any global AIDs that are also mutually supported by the chip card and the terminal in order for the merchant to have the greatest routing choice (the global brand network will be available on the Common U.S. Debit AID). Logic must be added to the terminal's software application to ensure that the mutually-supported Common U.S. Debit AID is selected in this situation.

The terminal will select the mutually supported Common U.S. Debit AID, and the transaction will proceed. The CVM will be selected based on what the card supports and the merchant's preference of Alternative 1 or Alternative 2 (refer to Section 3.5). The acquirer will use existing BIN tables or other existing logic to route the transaction as they do today.

If the terminal does not support the Common U.S. Debit AID that is on the card, and the card supports a global AID, the terminal will select a mutually supported global AID. Note that in this case, the transaction must be routed to the payment network associated with that global AID. This scenario is described in Section 4.6. If there is no mutually supported global AID, per EMV specifications the transaction must terminate.[9] This is not considered a fallback scenario, because the chip was read.

Rather than terminating the transaction, the terminal can generate a magnetic stripe transaction in order for the transaction to proceed. It is also possible for the acquirer host to set the terminal capability indicator in the transaction request to indicate that the terminal only supports magnetic stripe technology, so that the transaction does not appear to be fallback. Merchants should discuss this scenario with their payment network representatives to verify that this approach is permitted.

The scenario depicted below assumes that a Common U.S. Debit AID is supported by the chip card and the terminal.

[9] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3, November 2011, Book 1, Section 12.4

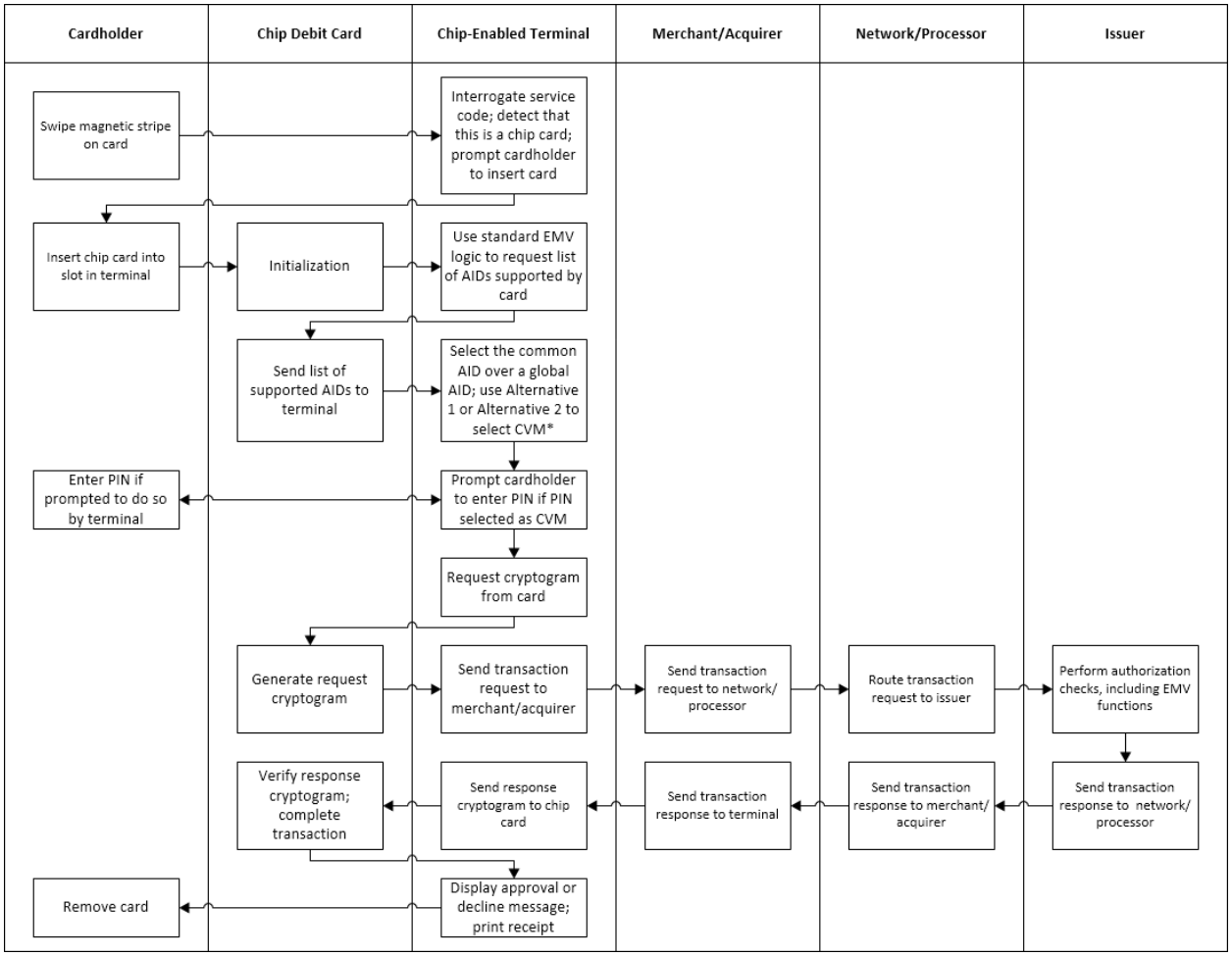

Figure 4-7

*Refer to Section 3.5 for more information about Alternative 1 and Alternative 2. Note that the Common U.S. Debit AIDs support Alternative 1 at this time.

4.8 Chip Debit Card with the DNA Shared Debit AID

A chip card containing the DNA Shared Debit AID (A0000006200620) will not have any other AID on the card. If the cardholder swipes the card, the terminal should detect that a chip card has been presented, and prompt the cardholder to insert the card. When the cardholder inserts the card, the terminal will communicate with the chip, and use standard EMV processing to select an AID that both the card and the terminal support.

If the terminal supports the DNA Shared Debit AID, that AID will be used to initiate the transaction. The CVM will be selected based on what the card supports, as described in Alternative 1 (refer to Section 3.5.1). The acquirer will use existing BIN tables or other existing logic to route the transaction as they do today.

If the terminal does not support the DNA Shared Debit AID, the DNA suggests that the terminal generate a magnetic stripe transaction in order for the transaction to proceed. It is also acceptable for the acquirer host to set the terminal capability indicator in the transaction request to indicate that the terminal only supports magnetic stripe technology, so that the transaction does not appear to be fallback.

The diagram below assumes the terminal does support the DNA Shared Debit AID. This example is similar to Figure 4-7 above.

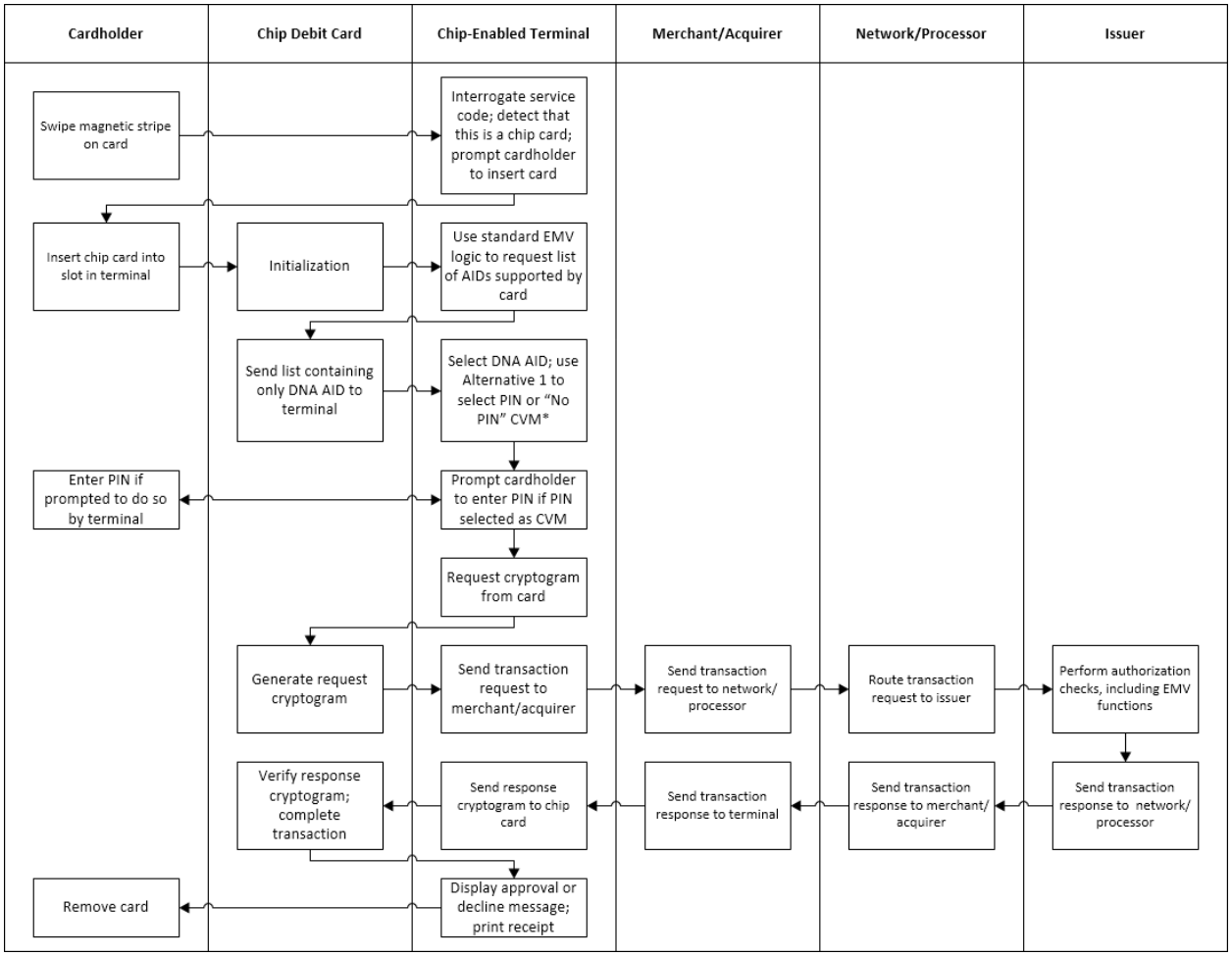

Figure 4-8

*Refer to Section 3.5.1 for more information about Alternative 1.

5 Impacts to Merchants

The information in this section is intended for merchants who plan to support global AIDs and the USDDAs in their POS terminals. This information is a guideline; each merchant should contact their terminal vendors and payment network representatives to determine what is required for their specific situation.

5.1 General Guidelines for EMV Implementation in POS Terminals

5.1.1 Technology

Merchants/terminal owners may be faced with a number of transaction scenarios involving different card technology (e.g., magnetic stripe, contact EMV, contactless magnetic stripe data/MSD, and contactless EMV) as well as different terminal technology (e.g., magnetic stripe, contact EMV, contactless MSD, and contactless EMV). This document focuses on contact EMV technology and (for purposes of transaction comparison and regression testing) legacy magnetic stripe technology.

Merchants/terminal owners need to determine whether to support contact chip cards, hybrid cards (cards with a magnetic stripe and a contact chip), contactless chip cards, dual interface cards, or a combination.

5.1.2 Hardware and Software

Merchants/terminal owners must ensure that each terminal has the appropriate hardware (e.g. slot for chip card insertion and chip card reader), EMV kernel, and application software to support EMV processing, and that the hardware and kernel have passed EMVCo Level 1 and Level 2 certification. It is the vendor's responsibility to perform these certifications, and to provide proof of certification to the terminal owner if requested to do so. Each merchant/terminal owner should work closely with their vendor to ensure that the kernel and application software provided by the vendor meet their business requirements. Contact your terminal vendor for additional details.

Some merchants may support one or more offline functions (offline PIN verification, offline card authentication, offline transaction authorization) in their terminals to ensure wide acceptance of non-U.S.-issued cards. These merchants should work closely with their acquirer and payment network to adhere to their requirements related to offline functions.

5.1.3 Configuration

When a payment card is presented to the POS terminal, the terminal must be able to detect whether it is a magnetic stripe card or a chip card. If the card is swiped, this is typically done by interrogating the first byte of the service code in Track 2. A value of 1 or 5 will indicate a magnetic stripe card; a value of 2 or 6 will indicate a chip card. (Refer to Appendix A.1 for the format of Track 2.) If the service code indicates that this is a magnetic stripe card, the terminal will continue to process the transaction "business as usual." If the service code indicates that this is a chip card, the terminal must prompt the cardholder to insert the card, so that the terminal can attempt to communicate with the chip. If a chip card is inserted, the terminal will attempt to communicate with the chip.

Merchants/terminal owners must determine which AIDs to add to the terminal configuration. The AIDs that will be supported by the terminal will be based on the business relationships the merchant has with the card brands and payment networks, and will include some combination of global AIDs, Common U.S. Debit AIDs, and the DNA Shared Debit AID. Global AIDs include those from the card brands, e.g. American Express, Discover, MasterCard, and Visa. Merchants/terminal owners in some geographical areas might also include AIDs for other networks such as JCB and UnionPay.

The table below shows examples of AIDs a merchant may need to support. The first four entries are considered U.S. Domestic Debit AIDs.

Payment Network	Product (Mnemonic)	AID
DNA Shared Debit AID	DNA Shared Debit AID	A0000006200620
Common U.S. Debit AID	Common U.S. Debit AID – Diners/Discover	A0000001524010
Common U.S. Debit AID	Common U.S. Debit AID – MasterCard Maestro	A0000000042203
Common U.S. Debit AID	Common U.S. Debit AID – Visa	A0000000980840
American Express	American Express	A00000002501
Diners Club/Discover	Discover	A0000001523010
JCB	Japan Credit Bureau	A0000000651010
MasterCard	MasterCard Credit or Debit	A0000000041010
MasterCard	Maestro (Debit)	A0000000043060
MasterCard	Cirrus	A0000000046000
Visa	Visa Credit or Debit	A0000000031010
Visa	Visa Electron	A0000000032010
Visa	Visa PLUS	A0000000038010

Figure 5-1: AIDs

No software changes should be needed to existing EMV kernels to support any of the AIDs shown in Figure 5-1. Any changes to an EMV kernel would require the vendor to re-certify that kernel (EMVCo Level 2 certification).

For each AID the terminal supports, the merchant must add the associated Terminal Action Codes (TACs) to the terminal configuration. TACs for the DNA Shared Debit AID are outlined in section 5.2 “Supporting the DNA Shared Debit AID.” Contact your global payment network representative to obtain the TACs for each of the global AIDs.

The terminal configuration must be updated to include the list of EMV Tags that are to be sent to the acquirer processor in a transaction request, and how they will be passed to the acquirer processor.

Per EMV specifications, a terminal should support the ability to allow the cardholder to select an application/AID or to confirm the application/AID proposed by the terminal[10]. The USDDA profiles are

[10] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3, November 2011, Book 1, Section 12.4

requiring the issuer to personalize their cards so that cardholder selection or confirmation is not required. However, merchants may need to support cardholder selection for international cards.

Merchants/terminal owners should contact their software vendor or processor to determine the specific changes that are required to terminal software, configuration, and downloads in order for a terminal to support EMV.

5.1.4 Messaging

Merchants may wish to consider additional signage on or around the terminal to assist the cardholder. Examples might include:

- An icon, sticker, or other indication that the terminal is chip-enabled.
- Arrows or other indicators that will help the cardholder find the slot for the chip card and understand the direction in which to insert the chip card.

Merchants may also wish to present additional messages on the terminal screen to assist the chip cardholder. Two examples of new messaging would be:

- If the cardholder swipes the card and the terminal detects that a chip card has been presented, the terminal must prompt the cardholder to insert the chip card.
- The terminal can display a "transaction processing – please wait" message while the card and the terminal are exchanging information. This exchange of information is a new step for chip card transaction processing, and may take a few seconds. The cardholder might believe nothing is happening during this very short time, and attempt to cancel the transaction and/or remove the card from the terminal prematurely.

	Because of the interaction that occurs between a chip card and a chip-enabled terminal at the beginning and at the end of a transaction, the chip card must remain in the terminal for the duration of the transaction. Until cardholders are familiar with this behavior, they may forget to remove the card in the terminal at the end of the transaction. Merchants can help cardholders by implementing a process to help the consumer remember to take their card at the appropriate time. This process might include messages on or around the screen, a beep, printing the receipt only after the card has been removed, or other steps the merchant feels are appropriate.

5.1.5 Global Card Brand Certifications

Terminal and host certifications are required by the card brands (American Express, Discover, MasterCard, and Visa). These certifications cover card-terminal interaction and functional testing. The purpose of these certifications is to ensure that terminals will perform according to the individual card brand's application/AID requirements, and that the acquirer can accept and pass EMV data according to the global payment network specifications. It is the merchant or terminal owner's responsibility to perform the card brand certifications; although in some cases they may be performed by the acquiring

processor. Terminal certification is performed after all software and configuration changes have been made, and all internal testing has been completed. This ensures that the combination of hardware, software, and configuration that is certified is exactly what is being placed into production. Contact your processor or global payment network representative for additional details regarding these certifications.

5.2 Supporting the DNA Shared Debit AID

The requirements for merchants who will support the DNA Shared Debit AID are summarized below.

A chip-enabled terminal supporting the DNA Shared Debit AID will:

- **Support contact chip and magnetic stripe technology**
- **Include the DNA Shared Debit AID (A0000006200620) in its list of AIDs**
- **Support online authorization**
- **Support online authentication**
- **Support online PIN, Signature (via No CVM flag) and No CVM**
- **Support the Terminal Action Codes (TACs) specified below**
- **Select the DNA Shared Debit AID when it is supported by the card and the terminal**

The DNA Shared Debit AID is a contact application; cards with the DNA Shared Debit AID will contain a contact chip and a magnetic stripe, therefore, merchants and terminal owners must support hybrid cards in order to support the DNA Shared Debit AID.

The DNA Shared Debit AID (A0000006200620) must be added to the list of supported AIDs in the terminal. The priority of the DNA Shared Debit AID in this list is not important, since a chip card containing the DNA Shared Debit AID will contain only that AID. The DNA Shared Debit AID will be selected by the terminal when both the chip card and the chip-enabled terminal support it, regardless of the priority of the DNA Shared Debit AID in the terminal.

The following Terminal Action Codes (TACs) must be configured for the DNA Shared Debit AID:

The TAC-Denial must contain a value of ’00 00 00 00 00’. This TAC Value instructs the terminal never to generate an offline denial of the transaction.

The TAC-Online must contain a value of ‘FC 50 BC F8 00’. This TAC Value instructs the terminal to generate an online authorization request whenever any of these conditions are met:

- Offline data authentication is not performed (SDA, DDA or CDA) or has failed
- The PAN is on the terminal exception file
- Cardholder verification is not performed or not successful
- Requested service not allowed for card product
- ICC application data are missing
- ICC application has expired
- Transaction exceeds the floor limit

- Terminal Velocity Checking indicate that the upper or lower consecutive offline limit is exceeded
- PIN Try limit is exceeded
- PIN entry is required, but PIN pad not present or not working
- PIN entry is bypassed
- Online PIN is entered
- The merchant forced the transaction online
- The transaction is selected randomly for online processing
- Terminal Velocity Checking indicates that no transaction has ever successfully been approved online

The TAC-Default must contain a value of 'FC 50 AC A0 00'. This TAC Value instructs the terminal to generate a decline if the transaction cannot be sent online for authorization whenever any of these conditions are met:

- Offline data authentication is not performed (SDA, DDA or CDA) or has failed
- The PAN is on the terminal exception file
- Cardholder verification is not performed or not successful
- Requested service not allowed for card product
- ICC application data are missing
- ICC application has expired
- Transaction exceeds the floor limit
- Terminal Velocity Checking indicate that the upper consecutive offline limit is exceeded
- PIN Try limit is exceeded
- PIN entry is bypassed
- Online PIN is entered
- The merchant forced the transaction online
- Terminal Velocity Checking indicates that no transaction has ever successfully been approved online

When the DNA Shared Debit AID is present, it will be the only AID on the chip card, so standard EMV Application Selection logic can be used to select the DNA Shared Debit AID.

The DNA Shared Debit AID does not support offline functions at this time.

Issuer Authentication will be optional for the DNA Shared Debit AID. This means that the chip card will accept a response from the issuer when no EMV data (e.g. the ARPC) is present in the transaction response message.

The DNA Shared Debit AID will not require the cardholder to confirm the AID selected by the terminal.

The DNA Shared Debit AID will not require issuer scripts in a transaction response message.

5.3 Supporting the U.S. Domestic Debit AIDs (USDDAs)

Based on business arrangements with card brands and payment networks, the merchant will add one or more of the USDDAs to their terminals. For example, if the merchant accepts MasterCard cards, the merchant will add the Common U.S. Debit MasterCard (Maestro) AID to the terminal. It is expected that most (and perhaps all) U.S. POS terminals will support all of the USDDAs.

For each AID the terminal supports, the merchant must add the associated Terminal Action Codes (TACs) to the terminal configuration. Contact your payment network representative to obtain the TACs for each of the USDDAs.

The terminal software must be modified to select a USDDA over a global AID, when both are supported by the chip card and the terminal. The table below shows the AID that the U.S. chip-enabled terminal must select in various scenarios, assuming that the terminal supports (at a minimum) the same AIDs the card supports.

Card Brand	Application(s)/AID(s) on Chip Card	U.S. Chip-Enabled Terminal Action
Discover	Discover Global AID	Select the Discover Global AID
Discover	Discover Global AID and Discover Common U.S. Debit AID	Select the Discover Common U.S. Debit AID
MasterCard	MasterCard Global AID	Select the MasterCard Global AID
MasterCard	MasterCard Global AID and MasterCard (Maestro) Common U.S. Debit AID	Select the MasterCard (Maestro) Common U.S. Debit AID
Visa	Visa Global AID	Select the Visa Global AID
Visa	Visa Global AID and Visa Common U.S. Debit AID	Select the Visa Common U.S. Debit AID
U.S. Debit	DNA Shared Debit AID	Select the DNA Shared Debit AID

Figure 5-2: AID Selection Scenarios

Merchants should carefully review the transaction scenarios depicted in Section 4 for more information about when and how a Common U.S. Debit AID will be selected.

If possible, terminals should be configured to include the AID (EMV Tag 9F06) that was selected by the terminal in the transaction request that is sent to the acquirer. Based on this information, the acquirer will be able to tell whether a global AID, a Common U.S. Debit AID, or the DNA Shared Debit AID was selected. Acquirers can use this information to assist with transaction routing.

When supporting a USDDA, merchants must implement the CVM alternative that best meets their business needs. Refer to Section 3.5 for a description of each alternative. Note that USDDAs use Alternative 1 at this time.

Merchants/terminal owners should contact their payment network representative to obtain specific certification requirements for that network's USDDA.

5.4 General Transaction Processing Considerations

Each merchant must decide how they will handle technical fallback (refer to Appendix A.9.1) and CVM fallback (refer to Appendix A.9.2), within payment network regulations.

The manner in which the chip is personalized can have a significant impact on the actions the terminal will take during transaction processing. For example, if the chip card is programmed to expect EMV data in the approved response from the issuer (i.e., Issuer Authentication is mandatory), several situations may arise that merchants need to be aware of. If issuers follow the guidelines for USDDAs, the scenarios described below should not occur when those AIDs are selected. Merchants may, however, be presented with cards where Issuer Authentication is mandatory, so merchants need to be aware of the following scenarios.

- If the chip expects, but does not receive, an ARPC in the approval response (i.e. Issuer Authentication is mandatory), the chip card will override the issuer's approval, and the transaction will be declined. The terminal will then generate a reversal for the issuer.
- If the chip card indicates that Issuer Authentication is mandatory for the selected AID, and the customer removes the card from the terminal before the approval response is received, the terminal will be unable to send the response cryptogram to the chip for verification; the terminal will send a reversal to the issuer when the approval response is received.

Merchants must obtain the current specifications from all networks or destination points to make sure it is clear what EMV data is supported by each specification, and where it must be placed within the messages exchanged between the terminal and the acquirer.

5.5 Education and Training

Merchants are faced with the challenge of educating their staff to have a basic knowledge of how a chip card is to be used at a chip-enabled terminal.

At a minimum, front-line staff will need guidance on the following:

- How to recognize a chip card
- When to swipe a card and when to insert a card
- When and how to instruct the customer to leave the card in the terminal until they are prompted by the terminal to remove the card
- How to interpret the various messages displayed by the terminal and explain them to the customer in order to complete the transaction

More complex challenges at the terminal may require the assistance of store management. Merchants need to determine the appropriate level of EMV education based on a staff member's responsibilities.

6 Impacts to Acquirers and Networks

The information in this section is intended for those who will be acquiring POS transactions that were initiated by a USDDA.

6.1 Transaction Processing Considerations

The implementation of EMV will require changes to existing acquiring routing processes.

6.1.1 "No CVM" Transaction Routing and Signature Capture Decision

The EMV Migration Forum's U.S. Debit EMV Technical Proposal recommends that acquirers support the "No CMV" (No PIN) CVM as described in Section 3.

In a "No CVM" transaction, it is important to identify which entity should make the decision as to whether to prompt for signature and capture, and how this is to be done.

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 document 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.

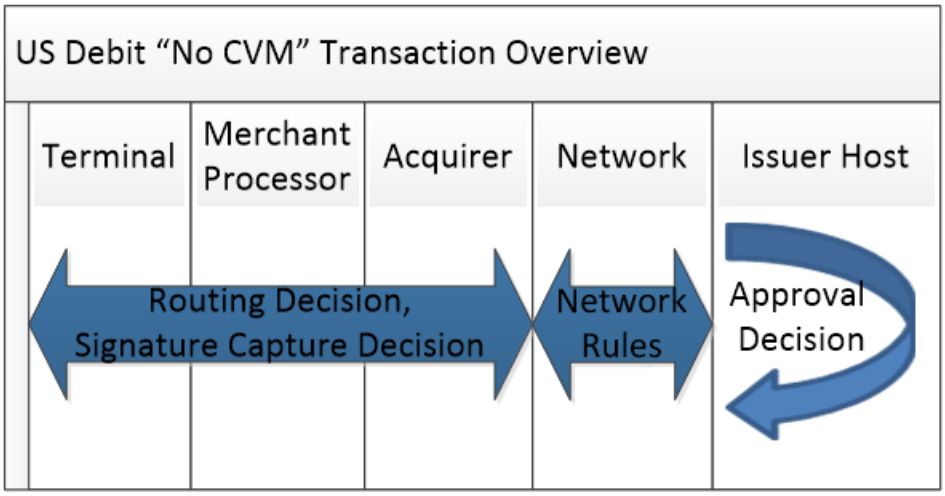

Figure 6-1: "No CMV" Transaction Overview[11]

6.1.2 Routing Table

One of the main reasons for the development of USDDAs was to allow acquirers and networks to continue to route transactions using existing rules and logic. This would indeed occur seamlessly and transparently ***if*** all acquirers and networks were chip-capable. But all acquirers and networks will not be chip-capable immediately, or at the same time. Meanwhile, many merchants, acquirers, and networks

[11] EMV Migration Forum Debit Technical Working Group U.S. Debit EMV Technical Proposal, Version 1.2, April 2014.

will be faced with the situation where a chip card is presented to a chip-enabled terminal, the chip is read successfully, and an EMV transaction is created, but the preferred destination (or perhaps all possible destinations) for the transaction are not yet ready to accept EMV data. In this case, the party that is attempting to deliver the transaction may have to choose between dropping the EMV data from the transaction in order to route it to the preferred destination, or selecting a different destination that is able to accept EMV data. There may be other options; the business relationships between the affected parties will drive the solution for those parties.

	A merchant, acquirer, or network must not drop EMV data from a transaction without an agreement between themselves and the non-EMV-compliant party, since the topic of liability comes into play. They must agree on who will bear the liability in the event of fraud: the party who dropped the EMV data from the transaction, or the party who required that action because they could not accept the EMV data.

Acquirers and networks may have default, or “black hole” routing, which must also be taken into consideration.

6.2 Certifications

Each payment network that is a member of the DNA is responsible for updating their network specifications to support EMV. These updates must support the functions of the DNA Shared Debit AID, for example:

- Support for online PIN verification
- Support for the “No CMV”
- Support for online authentication
- Support for online transaction authorization

The networks will provide their specifications to their partners. Each merchant or acquirer must work closely with their payment network representative to schedule certifications and other activities related to EMV implementation.

6.3 Education and Training

Acquirers and networks need to provide the appropriate level of education and training to internal staff as well as external partners.

7 Issuer Implementation and Impacts to Merchants

The information in this section is intended for issuers who plan to use a USDDA. Merchants may also find this information useful, because it provides information about chip cards containing these AIDs, and how the personalization of the chip card by the issuer can impact the choices made at and by the terminal during a transaction.

7.1 Chip Cards with a Common U.S. Debit AID

The information in this section provides general information about the Common U.S. Debit AIDs from Discover, MasterCard, and Visa. Contact each payment network representative for additional details about their Common U.S. Debit AID.

7.1.1 Requirements

As described in Section 3.3, U.S.-issued debit chip cards that are branded as Discover, MasterCard, or Visa will contain the Common U.S. Debit AID associated with that brand, and may also contain one or more global AIDs associated with that brand. A chip card that contains a Common U.S. Debit AID will contain only one Common U.S. Debit AID, although, as indicated above, that card may also contain one or more global AIDs.

For example, a U.S.-issued MasterCard debit chip card will contain the MasterCard (Maestro) Common U.S. Debit AID, and may also contain one or more global MasterCard AIDs (e.g., MasterCard Debit, MasterCard Cirrus).

Figure 5-2 in Section 5.2 contains examples of the combinations of AIDs that will likely be seen on U.S.-issued debit chip cards carrying a global brand. Note that each of these example chip cards will have a contact chip and a magnetic stripe. When a chip card containing one of the Common U.S. Debit AIDs is presented at a U.S. chip-enabled terminal, the Common U.S. Debit AID must be selected by the terminal in order to maintain routing choice for the merchant and acquirer.

Issuers must review their current card art and design to see if anything must change due to the placement of the contact chip. Issuers will not want the contact chip to hide important information such as the institution name or logo. Changes to card art and design may need to be approved by the payment network.

Discover, MasterCard and Visa have released profiles for their respective Common U.S. Debit AIDs. Please contact your payment network representative to obtain the related documentation.

7.1.2 Certifications

Each payment network has its own chip card certification process, in which some or all of the following individual certifications may be required:

- Chip hardware (EEPROM, ROM, cryptographic engine, memory protection logic)
    - Certification is typically performed or obtained by the card provider
- Operating system

  - MULTOS: certification is performed by EMVCo or MULTOS
  - Global Platform/Java: certification is performed by a qualified laboratory
  - Native/Card Vendor Proprietary: certification is performed by the card brand
- EMV application (e.g., Discover D-PAS, MasterCard M/Chip, Visa VIS)
  - Certification is performed by card brand or authorized third party
- Card Personalization Validation (CPV)
  - Certification is performed by issuer or their authorized agent; results are validated by card brand or certified third party
- Issuer host
  - Certification is performed by the issuer
- End-to-End
  - Certification is performed by the issuer

Please contact your payment network representative for specifics about their network's specific chip card certification process.

7.2 Chip Cards with the DNA Shared Debit AID

The information in this section pertains specifically to chip cards containing the DNA Shared Debit AID.

7.2.1 Requirements

The requirements for chip cards containing the DNA Shared Debit AID are summarized below.

	**A debit chip card containing the DNA Shared Debit AID will utilize the following profile:** ➢ **Will have a contact chip and a magnetic stripe** ➢ **Will contain the DNA Shared Debit AID and no other AID** ➢ **Will support online authorization** ➢ **Will support online authentication** ➢ **Will support online PIN and , Signature (via No CVM flag) and No CVM Will support the Issuer Action Codes (IACs) defined in the DNA Card Profile** ➢ **Will indicate that Issuer Authentication is Optional** ➢ **Issuer scripting is not applicable**

The DNA Shared Debit AID represents a contact application.

Issuers must review their current card art and design to see if anything must change due to the placement of the contact chip. Issuers will not want the contact chip to hide important information such as the institution name or logo. Changes to card art and design may need to be approved by the payment network.

Issuers need to determine what AID(s) their cards will support. A U.S.-issued debit chip card with a global brand (Discover, MasterCard, and Visa) will need to support the Common U.S. Debit AID associated with that global brand. A U.S.-issued chip card with the DNA Shared Debit AID

(A0000006200620) will contain only the DNA Shared Debit AID (i.e. no other AID). At this time, all U.S.-issued chip cards are expected to contain a magnetic stripe, so that the card can be used at terminals that are not yet chip-enabled.

As described in Section 3, chip cards containing the DNA Shared Debit AID will support online transaction authorization, online card authentication, and will support online PIN, and Signature (via No CVM flag) and No CVM. PIN verification will be supported online only. Chip cards with the DNA Shared Debit AID will not perform any offline verification, offline authentication, or offline authorization.

Chip cards with the DNA Shared AID will not require issuer scripting since all transactions are online.

The manner in which the chip is personalized has a significant impact on the actions the terminal will take during transaction processing. For example:

- Issuers must personalize the CVM list for each AID in the chip card to indicate the CVMs that AID supports, and the order of preference. For the DNA Shared Debit AID, the CVM List will include PIN, Signature (via No CVM flag) and No CVM as described in Section 3.5.1.
- Per EMV specifications, a chip card containing a single application may be personalized to require the cardholder to confirm the AID that is automatically selected by the terminal[12]. The DNA Shared Debit AID will not require cardholder confirmation.
- If the chip card is personalized so that it expects a response cryptogram to be sent with every approved transaction response (i.e. Issuer Authentication is mandatory), transactions may be declined by the card if the card does not receive this cryptogram. The chip will typically override issuer approval if it detects something amiss in the transaction response, e.g. a response cryptogram was expected but not received, or the response cryptogram cannot be verified. Therefore, Issuer Authentication must be set to Optional for the DNA Shared Debit AID. This will allow the transaction to be completed at the terminal even if no ARPC is received.

Please contact your debit network representative to obtain further details about the DNA AID card profile.

7.2.2 Certifications

Chip cards that contain the DNA Shared Debit AID must undergo the same hardware and operating system certifications as cards containing any global or Common U.S. Debit AID.

- Chip hardware (EEPROM, ROM, cryptographic engine, memory protection logic)
  - Certification is typically performed or obtained by the card provider
- Operating system
  - MULTOS: certification is performed by EMVCo or MULTOS
  - Global Platform/Java: certification is performed by a qualified laboratory

[12] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3, November 2011, Book 1, Section 12.4

- Native/Card Vendor Proprietary: certification is performed by the card brand

Chip cards that contain the DNA Shared Debit AID may use any application that conforms to the EMV Common Core Definition (CCD) specification and is compatible with the DNA Shared Debit AID card profile. The EMV application must be certified by the owner of the application.

Card Personalization Validation certification will ensure that the chip card conforms to the requirements of the DNA Shared Debit AID.

Please contact your debit network representative to obtain further details about the chip card certification requirements related to the DNA Shared Debit AID.

7.3 General Transaction Processing Considerations

Issuers will need to obtain current specifications from the payment networks in which they participate, to understand how EMV data is carried in each specification.

Issuers will need to determine whether they will perform EMV-related functions (e.g. verifying the ARQC and generating the ARPC), or if these functions will be performed by an on-behalf-of (OBO) party. An OBO party may perform these functions on a permanent basis, or only as a temporary measure until the issuer's host system has been upgraded, or only in a stand-in situation. The OBO party will need the keys that are required to verify and generate cryptograms and optionally generate issuer scripts for chip cards whose AIDs will accept scripts.

When implementing EMV (regardless of the AIDs supported), the issuer or OBO party must:

- Ensure that their Hardware Security Module (HSM) supports EMV-related commands
- Determine what, if any, new EMV-specific fields will be considered when making an authorization decision, and modify their authorization logic accordingly
- Be able to detect partial downgraded or fallback transactions and handle it according to payment network rules and issuer business practices
- Verify the ARQC and, if the transaction is approved, generate the ARPC, if required
- Make any required changes to existing fraud detection systems, e.g., new rules specifically for EMV transactions

The issuer or OBO party must also be aware of situations where a chip card is used at a chip-enabled terminal, an EMV transaction is generated, but somewhere along the transaction path the EMV data is dropped because the receiving party could not support EMV. This is sometimes referred to as partial downgrade. This scenario may happen until such time as all processors and networks in the U.S. support EMV. Issuers will need to decide how to handle (authorize or reject) these transactions, which are likely to have the following combination of information:

- The Track 2 Equivalent Data will be from the chip (because the chip was read); it will therefore not contain the CVV/CVC found in the magnetic stripe, however will contain the iCVV/iCVC value.
- The POS Entry Mode will indicate that the terminal was chip-enabled and the chip was successfully read
- The card security code (e.g., iCVV) from the chip may be present.
    - iCVV/iCVC will be present for partial downgrade transactions
    - CVV/CVC will be present for fallback transactions
- The Authorization Request Cryptogram (ARQC) will not be present

Issuers will also want to assess potential impacts to their OBO service provider, authorization platforms, back office and batch systems. For example, If an issuer wants to support partial downgrade and/or fallback transactions they will need to perform the following:

- Determine if their authorizing system can support these transaction types or use an OBO service provider.
- Ensure the card profile has the ARPC flag set to optional.
- Determine if iCVV/iCVC validation will be performed for partial downgrade transaction or CVV/CVC for fallback transactions.

7.4 Education and Training

Issuers will need to provide general EMV education as well as network-specific requirements to internal staff, particularly development, QA, and support.

Issuers are encouraged to provide information to their cardholders before and at the same time as they receive their chip card. It is important for cardholders to understand that there will be changes to the way they use their card at POS terminals. At magnetic stripe terminals, the chip card will typically be swiped; at chip-enabled terminals, the chip card will be inserted. The card insertion slot may be in a different location from one terminal to the next. It may not always be apparent that a terminal is chip-enabled, so cardholders should be prepared to follow the signage around, and prompts displayed by the terminal.

Each issuer should contact their payment network representative to obtain further guidance. The EMV Migration Forum also has some guidelines that may be of use to issuers. Refer to Section 9 for reference material.

8 Conclusion

Migrating to EMV can be a daunting prospect for any organization. The DNA aims to make the transition to EMV as simple as possible for its member organizations. We encourage you to work closely with your payment network representative to obtain their current EMV specifications and requirements, and to take advantage of other EMV-related materials that the DNA, your payment networks, and reputable industry organizations can provide. Together we can ensure a smooth transition to EMV.

9 References

9.1 EMVCo

Main page: www.emvco.com

EMV Specifications: http://www.emvco.com/specifications.aspx

A Guide to EMV: http://www.emvco.com/best_practices.aspx?id=217

9.2 EMV Migration Forum

Main page: www.emv-connection.com

Standardization of Terminology document: www.emv-connection.com/standardization-of-terminology/

EMV Testing and Certification White Paper: "Current U.S. Payment Brand Requirements for the Acquiring Community":

http://www.emv-connection.com/emv-testing-and-certification-acquiring-community-white-paper/

U.S. Debit EMV Technical Proposal white paper from the EMV Migration Forum Debit Technical Working Group: http://www.emv-connection.com/u-s-debit-emv-technical-proposal/

10 Glossary

AID (Application Identifier) An alphanumeric representation of the application defined within ISO 7816. A data label that differentiates payment systems and products. The card issuer uses the data label to identify an application on the card or terminal. Chip cards and chip-enabled terminals use AIDs to determine which applications are mutually supported, as both the card and the terminal must support the same AID to initiate a transaction. Both cards and terminals may support multiple AIDs. An AID consists of two components, a registered application identifier (RID) and a propriety application identifier extension (PIX). For additional details, refer to Appendix A.3.

Authorization Response Cryptogram (ARPC) A cryptogram generated by the issuer and sent in the authorization response back to the terminal. The terminal provides this cryptogram back to the chip card. This allows the chip card to verify the authenticity of the issuer response.

Authorization Request Cryptogram (ARQC) A cryptogram generated by the chip card at the end of the first round of card action analysis. The ARQC is included in the authorization request sent to the card issuer. This allows the card issuer to verify the authenticity of the card and the transaction request message.

BIN (Bank Identification Number) Typically a six digit number that identifies the institution that issued a card. Also known as the IIN (Issuer Identification Number). The BIN is the first part of the card number/PAN.

Chip card A device that includes an embedded secure integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory, or a secure memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, chip cards have the unique ability to securely store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication), and interact intelligently with a card reader. All EMV cards are chip cards.

Chip-enabled terminal A terminal that has, or is connected to, a chip card reader, an EMV application, and is able to process EMV transactions.

CVM (Cardholder Verification Method) In the context of a transaction, the method used to authenticate that the person presenting the card is the valid cardholder. EMV supports four CVMS: offline Personal Identification Number (PIN) (offline enciphered and plain text), online encrypted PIN, signature verification, and No CVM Required (“No CVM”). The issuer decides which CVM methods are supported by the card; the merchant chooses which CVMs are supported by the terminal. ATMs currently only support online PIN. The issuer sets a prioritized list of methods on the chip for verification of the cardholder.

DNA (Debit Network Alliance) An organization open to all debit networks whose goal is to facilitate U.S. EMV interoperability and acceptance of secure payment transactions. This is accomplished by a shared

governance model with input from all stakeholder communities, including merchants, issuers, and processors.

DNA Shared Debit AID Application identifier that is owned by all DNA members and is licensed by the DNA to other networks in a shared governance manner utilized by multi networks in a multilateral business arrangement.

EMV (EuroPay, MasterCard, Visa) Trademark referring to the three organizations that founded EMVCo. The EMV specification has evolved from a single, chip-based contact specification to include EMV Contactless, EMV Common Payment Application, EMV Card Personalization, and EMV Tokenization.

EMVCo An organization overseen by six member organizations (American Express, Discover, JCB, MasterCard, UnionPay, and Visa) and supported by many other payment industry stakeholders, whose goal is to facilitate worldwide interoperability and acceptance of secure payment transactions. This is accomplished by managing and evolving the EMV specifications and related testing processes.

Global Payment Network A payment network with a global (international) presence. In this document, this term is used to refer to American Express, Discover, MasterCard, and Visa.

ICC Integrated Circuit Card; see Chip card.

IIN (Issuer Identification Number) A six digit number that identifies the institution that issued a card. Also known as the BIN (Bank Identification Number). The IIN is the first part of the card number/PAN.

Magnetic Stripe A band of magnetic material used to store data. Data is stored by modifying the magnetism of magnetic particles on the magnetic material on a card, which is then read by a magnetic stripe reader.

PAN (Primary Account Number) The payment card number.

Payment Network A payment network provides POS and ATM services for credit, debit, ATM and prepaid card issuers and corresponding transaction acquirers. It establishes participation requirements, operating rules and technical specifications under a common brand(s) for the purpose of receiving, routing, securing authorization for, settling and reporting domestic and international payment transactions. Each payment network determines the types of transactions, payment devices and terminals that are permitted in its respective network.

PIN (Personal Identification Number) An alphanumeric code for 4 to 12 characters that is used to identify cardholders at a customer-activated PIN pad.

PIX (Proprietary Application Identifier Extension) The last digits of the AID that enable the application provider to differentiate between the different products they offer.

POS (Point of Sale) The place where a retail transaction is completed; the point at which a customer makes a payment to the merchant in exchange for goods and services.

RID (Registered Application Provider Identifier) First part of the Application Identifier (AID). Used to identify a payment system (card scheme) or network; e.g., MasterCard, Visa, Interac.

TAC (Terminal Action Code) Codes placed in the terminal software by the acquirer that indicate the acquirer's preferences for approving transactions offline, declining transactions offline, and sending transactions online to the issuer based on risk management performed.

Tag Values involved in an EMV transaction (which result from the issuer's implementation choices) are transported and identified by a tag which defines the meaning of the value, the format, and the length. The tag is simply a set of characters that identify the meaning of each piece of data transmitted between the ICC and the terminal.

U.S. Common Debit AID Application identifiers that are utilized by multi networks in a bilateral business arrangement. U.S. Common Debit AIDs are usually licensed by their global brand owners.

U.S. Domestic Debit AID (USDDA) Application identifiers that are utilized by multi networks in either a bilateral or multilateral business arrangement. The Common U.S. Debit AIDs and the DNA Shared Debit AID are examples of USDDAs.

Appendix A: Fundamental EMV Concepts

This section will introduce some basic EMV concepts which are referenced in this document. DNA-specific requirements are covered earlier in this document.

A.1 A Brief History of EMV and EMVCo

It has been more than 50 years since a magnetized strip of tape was first successfully attached to a plastic card. By the 1980s, standards had been established so that all payment-accepting devices knew what tracks could be found on a magnetic stripe card, the location of those tracks, and the format of the data within the tracks (shown below).

Track 1

- Maximum of 79 characters
- Format: %B[PrimaryAccountNumber]^[Name]^[ExpDate][ServiceCode][DiscretionaryData]

Track 2

- Maximum of 40 characters
- Format: ;[PrimaryAccountNumber]=[ExpDate][ServiceCode][DiscretionaryData]

Track 3

- Maximum of 107 characters
- Not used by most financial applications

While technology in most other industries has evolved, often quite rapidly (consider the changes to telephones, televisions, and cars in the past 50 years!), the magnetic stripe has remained basically unchanged.

All of us are accustomed to swiping a magnetic stripe card at a POS terminal. The terminal captures data from the magnetic stripe, and uses it as the basis for a transaction request. This relatively simple technology has served us well for many years.

But this fast and simple process has a downside: the magnetic stripe holds a limited amount of data, and it is static data. It is very easy for criminals to capture the track data from a card (through a technique known as “skimming”) and use this data to create a counterfeit magnetic stripe card. It can be very difficult for an issuer to detect fraud perpetrated by these counterfeit cards.

In the early 1990s, counterfeit card fraud was on the rise in Europe. Telecommunications were undependable in many areas, and merchants were unable to send transactions online for authorization by the issuer; therefore, many transactions were approved offline by the merchant. As a result, payments industry stakeholders realized they needed a way to ensure the legitimacy of a payment card when it was presented to the payment terminal. The limited amount of static data stored in the magnetic stripe did not lend itself to this type of authentication.

By this time, Europe was already using chip card technology, primarily for phones. It was clear to payments industry stakeholders that the chip provided a better platform for enhanced authentication than the magnetic stripe, for several reasons.

- A chip can store a great deal more information than a magnetic stripe.
- The chip is actually a miniature computer, sometimes called a microprocessor or secure microcontroller. Like a personal computer or laptop, the chip contains an operating system, memory, hardware and software security features, and a way to communicate with the "outside world."
- A chip can contain cryptographic modules, which are capable of encrypting and decrypting sensitive data.

Regional specifications were developed to provide guidance for implementation of chip technology. Within a given region, chip cards and terminals would follow that region's specification, but when cards were taken to a different region, they were incompatible with the terminals in that region. For cardholders traveling outside of their own country, this silo approach was obviously not acceptable.

In 1994, a working group was formed by Europay, MasterCard, and Visa, the three primary payment networks in Europe at that time (hence the acronym EMV). This working group, which became known as EMVCo, established standards and specifications to facilitate global interoperability and compatibility of chip-based payment cards and payment card-accepting devices. Today EMVCo is jointly owned by American Express, Discover, JCB, MasterCard, Union Pay, and Visa. EMVCo publishes specifications for contact chip cards, contactless cards, and EMV contactless mobile payments. The specifications are free and can be downloaded from www.emvco.com.

The EMVCo specifications provide a framework for EMV implementation. They address the requirements for the chip card reader (also known as the Interface Module, or IFM) and the kernel (a software component that is responsible for communicating directly with the chip in "machine language"). The EMVCo specifications define the format of commands to be sent by the terminal to the chip and the response returned by the chip. The EMV specifications do not, however, address the specific requirements of any payment network. Therefore, each of the global payment networks created chip specifications that are based on the EMVCo specifications but also satisfy their individual operating rules, regulations, and processes. As a result, the chip specifications from the global payment networks (American Express, Discover, MasterCard, and Visa) contain many similarities, but also some significant differences.

A.2 Magnetic Stripe Compared to EMV

With an online magnetic stripe transaction, the customer typically swipes the card through the POS terminal (1). The terminal formats a request message, which is sent to the acquirer (2), and on to the network (3), then the issuer (4). The issuer makes an authorization decision and generates a response message (5), which goes to the network (6), then acquirer (7) and then to the terminal (8). There is no further interaction between the terminal and the magnetic stripe card after the card is initially swiped.

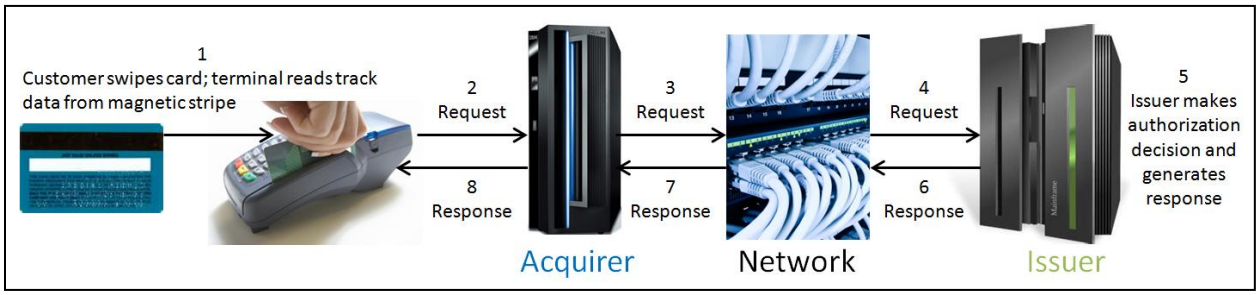

Figure A-1: Online POS Magnetic Stripe Transaction Flow

With an online POS EMV transaction, the customer inserts the chip card into the chip-enabled POS terminal and leaves it there for the duration of the transaction. The card and the terminal interact, exchange information, and make several decisions. The card generates a request cryptogram (1). The terminal formats a request message, which contains the same fields the magnetic stripe transaction request message contains, plus some new, EMV-specific data, including the request cryptogram. The request message is sent to the acquirer (2), the network (3), and then to the issuer (4). The issuer validates the cryptogram, makes an authorization decision, generates a response cryptogram, and potentially generates issuer scripts containing commands with minor updates to the chip (5). The response message is sent to the network (6), then the acquirer (7) and then to the terminal (8). The terminal passes the response cryptogram and issuer scripts to the chip, which validates the cryptogram and executes commands in the issuer scripts (9). When the transaction is complete, the terminal prompts the customer to remove the card.

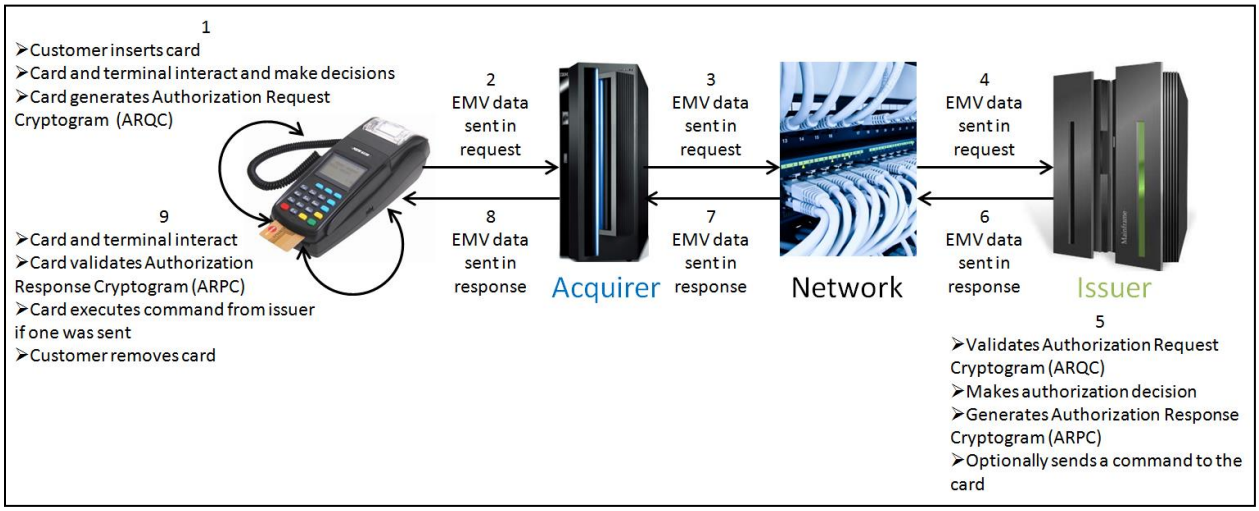

Figure A-2: Online POS EMV Transaction Flow

The following chart summarizes the major differences between an online magnetic stripe transaction performed by a magnetic stripe card at a magnetic stripe POS terminal and an online EMV (chip) transaction performed by a chip card at a chip-enabled POS terminal.

Magnetic Stripe Transaction	EMV (Chip) Transaction
Card is typically swiped and returned to cardholder after magnetic stripe data has been read*	Card must be inserted and remain in the terminal for the duration of the transaction
There is no interaction between the card and the terminal after magnetic stripe has been read	Data is exchanged between the card and the terminal to initiate the transaction
Card does not generate a cryptogram	Chip card generates a unique cryptogram which is sent to the host for verification; by verifying this cryptogram, the issuer ensures that the transaction was initiated by a legitimate card
Online request message contains no EMV-specific data	Additional EMV-specific data is in the online request message
Host does not perform any EMV-related processing	Additional processing is required by host to verify the request cryptogram, interrogate additional EMV-specific fields in the request message, generate a response cryptogram, and optionally generate an issuer script containing instructions for the chip
Online response message contains no EMV-specific data	Online response message may contain EMV-specific data, e.g. a response cryptogram and an issuer script
There is no interaction between card and terminal at the end of the transaction	Data is exchanged between card and terminal at the end of the transaction

Figure A-3: Magnetic Stripe Transaction and EMV (Chip) Transaction Comparison

*Some merchants have terminals where the card is not swiped, but instead is inserted and may not be immediately returned to the cardholder (e.g., Target stores).

A.3 Applications and AIDs

A cardholder may have multiple magnetic stripe cards in their wallet: debit cards, credit cards, loyalty cards, gift cards, etc. The cards will have different card numbers (PANs), and each card owned by a single cardholder may be associated with a unique account.

Because the chip is able to store so much more data than a magnetic stripe, it is possible to house multiple products or programs in a single chip. For example, a single chip can house a debit application and a credit application, or two debit applications. These applications may work differently; for example, a debit application may require the use of a PIN whereas a credit application may prefer the use of signature, which means that the data and logic associated with a debit application may be different from the data and logic associated with a credit application. Within the chip, this is easily accommodated by segregating the data and logic for one application from the data and logic for another application. This is simply not possible within the magnetic stripe on a payment card.

A software application for a specific product that resides on a chip card is known as an "ICC (Integrated Circuit Card) application" (also referred to as the "card application" or "chip application"). The ICC application contains the logic and parameters that are used during the interaction between the card and the terminal when a payment transaction is initiated.

Each ICC application is represented by an Application Identifier, or AID. Every AID is assigned by the ISO/IEC 7816-5 registration authority, and must conform to ISO/IEC 7816-4. The AID has a specific format, consisting of:

- The Registered Application Provider Identifier (RID), which identifies the payment network that provides the application, and
- The Proprietary Application Identifier Extension (PIX), which identifies the specific program or product offered by that payment network.

Refer to Figure 5-1 in Section 5 for a list of the ICC applications and their associated AIDs that are likely to be seen at U.S. chip-enabled terminals.

The AIDs are usually referred to by their product name, or mnemonic. As an example, the AID "A00000002501"is associated with the mnemonic "American Express." The ICC applications, with their corresponding AIDs, are written onto the chip during card production. A chip card may contain multiple applications and associated AIDs; in this case, the issuer is expected to indicate the priority of each application/AID on the card. When there is more than one application on the card, the issuer has the option of configuring an application so that the terminal will prompt the cardholder to select the desired application. The issuer may also require the terminal to confirm the application that is automatically selected by the terminal. Note that although these options are supported by EMV, they may not be required by a specific AID, such as the DNA Shared Debit AID. However, this information highlights the types of differences that may be seen between AIDs in a single chip.

As indicated in Figure A-2 above, a chip-enabled terminal will request information from the chip card at the beginning of a transaction. Based on the information provided by the chip card, the terminal is able to identify the applications and networks the card supports, the owner of each application, the risk management parameters for that application, and other information that will be used to generate the transaction request.

Each chip-enabled terminal will contain a list of the AIDs that it supports. These AIDs represent the payment networks with which the terminal owner, merchant, or acquirer is affiliated. Because of the differences between the network chip specifications, it is critical that at least one AID be mutually supported by the chip-enabled terminal and the chip card in order for a transaction to proceed.

The process whereby the cardholder selects the application, or the terminal selects the highest priority, mutually supported application (by AID), to use for transaction processing is known as Application Selection. Per the EMVCo specification: "If there are no mutually supported applications, the transaction is terminated."[13]

For a chip card that might be used outside of the U.S., a U.S. issuer will include at least one global AID in that chip card. Within the U.S., for debit cards, the issuer may decide to use a Common U.S. Debit AID or the DNA Shared Debit AID in order to be Durbin compliant and preserve current routing choice. Refer to Section 3 for more information about the Common U.S. Debit AIDs and the DNA Shared Debit AID.

A.4 Chip Card Technology

The EMV chip does not have a built-in power supply, such as a battery. The power to drive the chip is provided by the card reader. This can be done in several ways, depending on the card interface (contact or contactless).

A.4.1 Contact EMV

With a contact chip card, the contact plate is actually visible on the face of the card. There are very stringent specifications for the location of the chip on the card, because the chip must come into physical contact with the card reader. Each contact point on the top of the chip is assigned a specific function, such as ground, input/output, clock, reset, and supply voltage, so it is vital that the contact points line up correctly with the corresponding points in the card reader.

The chip is powered up when the plates in the chip come into physical contact with the chip card reader. The power is supplied by the terminal and the chip card reader.

[13] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3, November 2011, Book 1, Section 12.4

Figure A-4: Contact Chip Card

The term "hybrid card" is used to refer to a card that is equipped with both a magnetic stripe and a contact chip interface, where the chip carries an ICC application that supports the same payment product that is encoded on the magnetic stripe.

Many issuers begin their foray into chip technology by issuing hybrid cards. Although some regions of the world have planned to eliminate the magnetic stripe from their cards within the next few years, it is likely that the U.S. will produce and support hybrid cards for a number of years to come.

Virtually every chip-enabled terminal can communicate with a hybrid card, using either the chip or the magnetic stripe. The chips for these cards are typically cheaper than those used in dual-interface cards (see Appendix A.4.3) because they require less memory. There is a single interface technology to test (the contact interface). However, these cards must be re-issued in order to add contactless functionality.

A.4.2 Contactless EMV

With a contactless card, the chip is not visible on the exterior of the card. It is actually embedded between the layers of card material.

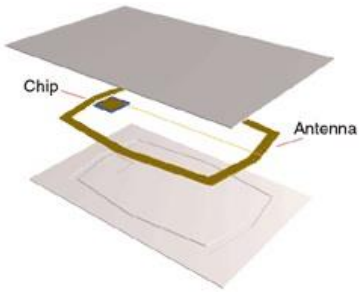

Figure A-5: Contactless Chip Card

The chip is powered up when it comes within the "excite" or "polling" field of a terminal that has a contactless interface. When a card with a contactless interface is presented to the terminal, the terminal will attempt to power up the chip and begin communicating with the card. The radio frequency (RF) waves that are used for this communication will only operate at a distance of 2-4," because they must support the exchange of large amounts of data, and they must be able to handle the cryptography associated with contactless technology. Contactless cards are sometimes referred to as "proximity"

cards, because they must be in close proximity to the terminal in order to communicate with the terminal.

Contactless technology is very popular for applications such as physical access to buildings, where being outdoors may make it inadvisable to use contact cards due to rain, snow, or extremes of temperature. It is also popular in industries where speed and convenience are critical, such as transit.

But many payment devices do not have a contactless interface, so issuers usually do not produce chip payment cards that have only a contactless interface.

Terminals that support contactless cards will have the logo shown below on the left below. Cards that have a contactless interface will have the logo shown below on the right below.

Contactless logo for terminals Contactless logo for cards

Figure A-6: Contactless Logos

There are two contactless modes of operation: mag-stripe mode and EMV mode.

With contactless mag-stripe mode (also known as contactless Magnetic Stripe Data, or contactless MSD), the chip in the card will generate a cryptogram, but the transaction request message generated by the terminal is still in the current magnetic stripe format, which has no room for the cryptogram. Instead, part of the discretionary data in the Track 2 is replaced with limited data from the chip, including the chip card security code (e.g., iCVV, Chip CVC, iCSC). This data allows the issuer to verify the authenticity of the card, even without a cryptogram.

With EMV mode, the chip-enabled terminal generates a transaction request message that can carry the new EMV data generated by the card and the terminal, including the cryptogram generated by the chip.

A.4.3 Dual Interface Cards

The dual interface card represents the best of both worlds. This chip card contains a magnetic stripe, plus a single chip that supports both contact and contactless ICC applications. The chip is connected to an antenna to facilitate contactless communication. These cards can communicate with virtually any chip-enabled terminal, through the magnetic stripe, the contact interface, or the contactless interface, depending on what the terminal supports.

Figure A-7: Dual-Interface Card

Dual interface cards provide many benefits, but they are more expensive than contact chip cards. Extra testing is required, because all functions for the contact interface and the contactless interface must be tested, in addition to regression testing of the magnetic stripe. Therefore, it can take longer to get these cards into production. When contactless applications support offline functionality, these cards must also support Public Key Infrastructure, so additional keys and certificates are required for these cards. However, factors such as consumer demand and emerging payment trends should be weighed when considering dual interface cards. It is important to note that the Common U.S. Debit AIDs and the DNA Shared Debit AID support only contact applications at this time.

A.5 Online vs. Offline

The terms “online” and “offline” have certain connotations within the magnetic stripe environment. The use of these terms in relation to EMV may be slightly different from the way they are used today by the U.S. payments industry.

The term “online” reflects online communication with the acquirer (or its agent); the acquirer is assumed to be capable of communicating with a payment network or directly with the issuer. The use of the term “online” assumes that some type of data will be verified by a host system, for example, an issuer’s authorization system. The EMV specification supports online PIN verification, online card authentication, and online transaction authorization. These terms are discussed in more detail below.

The term “offline” is used to indicate that some type of data is verified between the chip card and the chip-enabled terminal, and, if the verification is successful, that data is not sent to a host system if the transaction goes online. Several offline functions can be implemented at the Point of Sale, although currently no offline functions are supported at ATMs. The EMV specification supports offline PIN verification, offline card authentication, and offline transaction authorization at POS terminals. These terms are discussed in more detail below.

As previously noted, one of the main drivers behind the development of EMV in the 1990s was the ability to support offline functions. As a result, many regions around the world support offline functions in chip cards and at chip-enabled POS terminals. The U.S. operates in an almost 100% online environment, so many U.S. issuers may not provide offline functions in their chip cards, except for cardholders who travel to other countries where this functionality may be useful.

A.5.1 Online and Offline Functions in the U.S.

The following information provides a perspective of support for offline functions in the U.S.

American Express: All Amex transactions initiated at U.S. POS terminals will go online for authorization. Other regions that support offline processing will have floor limits that vary based on market. All AXP-issued cards (globally) will work, regardless of the terminal settings, because the card can always request to go online to obtain approval, even when the transaction amount is below the floor limit.

Discover: Offline data authentication is not required at online-only terminals.

DNA: Offline functions will not be supported at this time. All transactions initiated from the DNA Shared Debit AID will go online for PIN verification, card authentication, and authorization.

MasterCard: Debit MasterCard cards, Maestro cards, and applications identified with the Maestro Common U.S. Debit AID may be configured as online-only cards. Offline functions are not required to be supported. In the POS terminal, the floor limit may be set to $0 to force all transactions to go online.

Visa: All Visa cards can be authorized online. No Visa card that conforms to Visa rules requires offline authentication for online transactions. Visa encourages and promotes online-only terminals.

A.6 Authorization

The term "authorization" refers to the process whereby an issuer (or organization acting on behalf of the issuer) decides whether to approve or decline a transaction. Issuers have complex authorization logic in place today, which must be enhanced to support new EMV-specific data and functions. Refer to Section 7 for more information about impacts to issuers.

It is expected that virtually all transactions initiated at U.S. POS terminals will be sent online for authorization.

A.7 Authentication

"Authentication" refers to the process of proving that an object, data, or identity is genuine. In the payments industry, counterfeit card fraud is growing rapidly. EMV is a proven method of ensuring that a legitimate card was used to initiate a transaction, i.e. authenticating the card that was used to initiate a transaction. This is accomplished when the card generates a cryptogram for each transaction, and the cryptogram is then verified.

There are two main card authentication methods (CAM):

- Online CAM, where the issuer verifies the cryptogram as part of online authorization
- Offline CAM, which is performed by the terminal

All U.S.-issued chip cards are expected to support online authentication; some cards (typically those issued to international travelers) may also support offline authentication. There are several offline data authentication methods.

Some merchants may include support for offline authentication in their terminals to ensure greater acceptance of non-U.S.-issued chip cards in the event that the link to the acquirer or network is unavailable.

A.8 Cardholder Verification Methods

Cardholder Verification is the process used to confirm that the person presenting the card is the genuine cardholder. Magnetic stripe technology supports several Cardholder Verification Methods (CVMs): online PIN, signature, and No CVM Required (often called "No CVM"). Each payment network has its own rules related to the CVM(s) it supports.

Cardholders are already accustomed to signing a paper receipt or the electronic signature pad at U.S. POS terminals. For low-value transactions, cardholders are accustomed to making their purchase without entering a PIN or a signature (i.e. No CVM Required). When a PIN pad is present and a PIN is required for the transaction, some cardholders may also be accustomed to entering a PIN at the POS. EMV supports online PIN verification, signature, and "No CVM."

EMV also supports offline PIN verification. Issuers wishing to implement offline PIN verification must store the PIN in the chip. The PIN entered by the cardholder at the terminal is compared to the offline PIN stored in the chip, so the PIN is not sent online to the host for verification. Offline PIN is the preferred CVM in some countries, but because almost all U.S. transactions go online to a host system for authorization, many U.S. issuers may feel that it is not worth the additional effort and expense to support offline PIN in the majority of their chip cards. Exceptions may be made for chip cards issued to international travelers.

Some merchants may include support for offline PIN verification in their terminals to ensure greater acceptance of non-U.S.-issued chip cards in the event that the link to the acquirer or network is unavailable.

For an in-depth discussion of Cardholder Verification Methods and their use with the Common U.S. Debit AIDs, please refer to the EMV Migration Forum Debit Technical Working Group's U.S. Debit EMV Technical Proposal.

For additional information on CVMs and the DNA Shared Debit AID, refer to Section 3.

A.9 Fallback

There are two types of fallback: technical fallback, and CVM fallback.

A.9.1 Technical Fallback

Technical fallback, commonly referred to simply as fallback, refers to the scenario when a chip card is presented to a chip-enabled terminal, but for some reason the chip cannot be read. The terminal then generates a magnetic stripe transaction based on the data in the magnetic stripe on the card.

There are legitimate reasons this can happen; for example, the chip is scratched, or the card reader's contacts are dirty and cannot make contact with the contact plate on the card. But fallback can also be

indicative of fraud. As long as a card has a magnetic stripe on it, the data from the magnetic stripe can be skimmed, and placed on a counterfeit card. If the data was skimmed from the magnetic stripe on a chip card, the terminal will read the magnetic stripe and then attempt to read the chip. Since there is no chip on the card, the terminal will typically generate a "fallback" magnetic stripe transaction using the data from the magnetic stripe. Merchants and acquirers must contact their individual payment networks to obtain their requirements related to fallback.

A.9.2 CVM Fallback

CVM fallback refers to the situation where the preferred CVM cannot be used, and a different CVM, usually signature, is used instead. Two of the scenarios when CVM fallback can occur are:

- The cardholder or merchant uses the PIN bypass function which is available on some terminals
- The terminal's PIN pad is inoperable

In either case, CVM fallback to signature or "No CVM" may be allowed if the issuer's preferred CVM is online PIN or offline PIN. Issuers and merchants must refer to the individual payment networks for their CVM fallback requirements.

CVM fallback may not be common in the U.S., since offline PIN verification may not be supported in most U.S.-issued chip cards, and some cards may not require a PIN for a transaction. However, merchants may see instances of CVM fallback when presented with globally branded cards issued outside of the U.S.

Appendix B: Debit Technical Proposal Alternative 2

This alternative is based on a Common U.S. Debit AID on a chip card that reflects all CVMs that are generally available under the EMVCo specifications based on a particular card's combination of supported networks. The chip card's CVM List will make a distinction between the two "No CVM" options (i.e. signature and "No PIN"). Standard EMV processing will be used to perform signature debit transactions originating from U.S. terminals under a signature CVM. Issuers would configure their Common U.S. Debit 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.

An example of the user of Alternative 2 is as follows. If a chip card supports two networks where network 'A' supports signature and online PIN, and network 'B' supports online PIN and "No CVM", all enabled for domestic transactions, the card's Common U.S. Debit AID or DNA Shared Debit AID would reflect the union of all of the supported CVMs across all affiliated networks: signature, online PIN, and "No CVM".

From a technological perspective, the only difference between Alternative 1 (described in Section 3.5.1) and Alternative 2 is that under Alternative 2 the chip card can have **both** signature and "No CVM" in the chip card's CVM List. The terminal can support either signature CVM or "No CVM" or both. Depending on what was chosen, the host decisioning as to which CVM actually applies to the transaction would still hold.

Alternative 2 was developed to satisfy the needs of issuers and networks desiring to use all three distinct CVMs. As of July 2014, this alternative is not supported by any Common U.S. Debit AID or the DNA Shared Debit AID.

The diagram below presents further details on how the processing would work using Alternative 2.

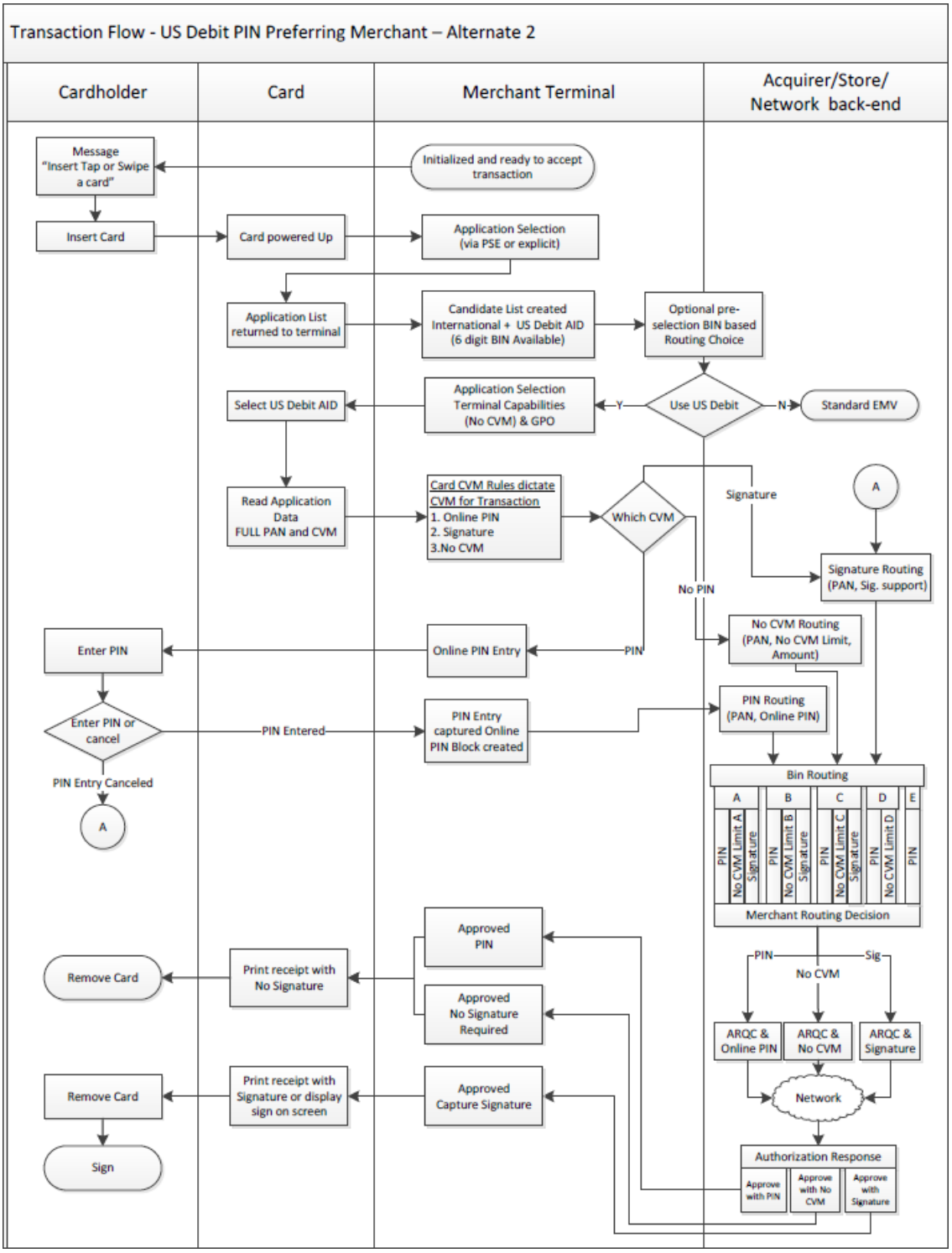

Figure B-1: CVM Alternative 2

For further information, please refer to the U.S. Debit EMV Technical Proposal, Section 3.3.2.