Implementing EMV®at the ATM:

Requirements and Recommendations for the U.S. ATM Community

Version 1.0

Date: August 2014

About the EMV Migration Forum

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

EMV is a trademark owned by EMVCo LLC.

TABLE OF CONTENTS

1 Introduction

1.1 Executive Summary

ATMs are an important component of the move to EMV payment technology, commonly known as "chip" payment technology.

For point-of-sale (POS) devices, the impetus for conversion to chip rests primarily on two foundations: fraud control and multi-application support for value-added functions (such as loyalty programs or vouchers). For ATMs, however, always-online authorization, coupled with the use of a PIN, and the relatively higher security environment, has historically resulted in lower levels of fraud compared to POS. Further, as a financial services machine, the ATM has not been an attractive opportunity to offer extensive value-added functionality.

Both factors are beginning to change for the ATM. Magnetic stripe skimming, combined with PIN capture (via shoulder-surfing, pinhole cameras, and false fronts), has led to rapid increases in ATM fraud rates. In some markets, this rise in fraud has led to aggressive programs for chip migration for ATM transactions. Meanwhile, the migration of ATMs to "kiosks," offering POS capability in addition to cash dispensing, has increased the potential for value-added functionality in ATMs.

Additionally, Discover, MasterCard, and Visa have published liability shift dates that impact ATM owners. A liability shift is not a mandate; ATM providers and acquirers are not being forced to migrate to EMV. However, the liability shift provides a very strong practical incentive to do so. (Refer to Section 5.2 for more information about the liability shifts.) Further, ATMs are seen as an important component of chip card management. ATMs are generally seen as a safer location to change/unlock PINs; to unblock, add, modify, and delete applications; to manage proprietary applications; and to execute lengthier and more complicated user scripts.

This document provides guidance to ATM providers, acquirers, processors, and vendors who are preparing to implement EMV at the ATM in the United States. It includes information about which functions must be implemented to provide EMV compliance at the ATM, as well as recommended planning activities for EMV implementation. Technical details about an EMV transaction are also included.

1.2 Notes and Information Disclosure

This document has been prepared by the EMV Migration Forum ATM Working Committee ("Working Committee"). The recommendations, suggestions and other guidance and information provided in this document ("Recommendations") represent the general consensus of the members of the Working Committee, following extensive research and discussion, and are provided solely as a general guide for the convenience of interested ATM industry constituents.

In the ATM context, and generally, implementation of EMV ultimately depends on the specific circumstances, environment and business needs of those involved. Prior to implementing EMV, it is therefore assumed (and the EMV Migration Forum strongly encourages and recommends) that implementers will independently and thoughtfully (i) assess their respective environments, requirements, challenges, preferences, business needs and related matters, and how the foregoing may impact their specific EMV implementation(s), (ii) consider the Recommendations provided in this document, and (iii) consult with appropriate acquirers, issuers, processors, vendors and payment network partners, and obtain the support and guidance of experienced and qualified professionals where appropriate.

Those who are primarily interested in the steps required to implement EMV at an ATM may wish to focus on the following sections of this document:

- Section 3: Basic EMV Requirements for ATMs
- Section 4: Migration Planning

More technical information about EMV can be found in the following sections:

- Section 2: Fundamental EMV Concepts
- Section 7: ATM Transaction Processing with EMV

1.3 Assumptions

- It is assumed that the reader is familiar with common, current practices with respect to the deployment and operation of ATMs in the U.S. This document specifically focuses on new requirements introduced by EMV, as these may not impact the provision of ATM service.
- This document is intended to be an overview and guide, not a comprehensive EMV textbook or step-by-step instruction manual. **Due to variations in hardware, and differing requirements of vendors and service providers, readers are directed to the references listed in Section 10, as well as their own vendors and partners, for additional information.**
- ATMs will always go online for Cash Disbursement and Balance Inquiry authorizations. For this reason, many of the EMV functions used to support offline functionality at the POS are not needed for Cash Disbursements and Balance Inquiries.
- "ATM Transactions" in this document are assumed to be "Cash Disbursements", as defined under EMV. Other ATM transaction types (e.g., Balance Inquiries, Deposits, Funds Transfers) are not considered EMV transactions[1]. These "Non Cash Transactions" are briefly discussed.
- Sales of goods or services at ATMs are not addressed in this document, as rules governing such sales vary widely across payment networks. Many ATM deployers are looking to sales or services at the ATM (e.g., top-ups, lottery, quasi-cash) as a way to enhance revenue and hence the commercial viability of the location. Because these transactions require additional considerations, particularly when performing certification, implementation details should be addressed with the specific acquiring processor, sponsor bank and network involved.

[1] These transaction types can use EMV functions and can be initiated using the EMV chip. However, they will not go through all stages of EMV processing.

2 Fundamental EMV Concepts

This section will introduce some basic EMV concepts which are referenced in subsequent sections of the document.

2.1 Comparing a Magnetic Stripe Transaction with an EMV Transaction

The following chart highlights the major differences between a magnetic stripe transaction performed at an ATM in the U.S. today, and an EMV transaction performed at an ATM in the U.S. following implementation of EMV by the ATM operators and processors. Refer to Section 7 for more information.

Magnetic Stripe Transaction	EMV Transaction
Card is swiped, inserted, or dipped, and is 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 card and terminal after magnetic stripe has been read	Data is exchanged between card and 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
Online request message contains no EMV-specific data	Online request message contains additional EMV-specific data
Host does not perform any EMV-related processing	Additional processing is required by host to verify request cryptogram, generate response cryptogram, and interrogate additional EMV-specific fields in the request message
Online response message contains no EMV-specific data	Online response message contains additional EMV-specific data
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

Diagram 2-1

2.2 EMV and EMVCo

Europe began experimenting with chip card technology in the early 1980s. It quickly became clear that standards were needed to ensure that any chip card used for payments would be compatible with any chip-enabled payment-accepting device. So in 1994, a working group was established by Europay, MasterCard, and Visa, the three primary payment associations in Europe at that time, hence the acronym EMV. This group formed EMVCo, whose purpose was to develop standards and specifications that facilitate global interoperability and compatibility of chip-based payment cards and chip-card-accepting devices. EMVCo (www.emvco.com) is currently owned by American Express, Discover, JCB, MasterCard, UnionPay and Visa.

The EMV specifications are the foundation for all financial applications that utilize chip technology and are intended to be interoperable across many participants. While some discussions may refer to “EMV-

approved devices" or "EMV-approved ATMs", the EMV specifications only apply to two areas of the ATM: the InterFace Module and the kernel. Thus strictly speaking, an "EMV-approved device" is one that contains both an EMV-approved InterFace Module and an EMV-approved kernel.

2.2.1 Chip Reader

In EMV terminology, a chip "reader" is known as an InterFace Module (IFM). EMV Level 1 terminal type approval is intended to test and validate that the IFM conforms to Level 1 of the EMV mechanical and electrical protocol specifications, which cover the transfer of data between the terminal and the card. For more information about chip readers, refer to Section 3.1 of this document.

2.2.2 Kernel

The software component that implements EMV functionality is known as the EMV application kernel, or simply the kernel. EMV Level 2 terminal type approval is intended to test and validate that the software that performs the EMV processing, referred to as the EMV Level 2 kernel, conforms to the EMV specifications. For more information about the EMV kernel, refer to Section 3.4 of this document.

2.2.3 Approval and Renewal Processes

EMV chip readers (IFMs) and software kernels are submitted for testing, normally by the vendors, to one of a number of EMVCo-approved laboratories. The laboratories will then test the IFMs and kernels against appropriate test scripts as defined by EMVCo. These test scripts are updated annually to address situations that have arisen during deployments or have been uncovered in laboratory analysis. In the late 1990s, the Level 2 (kernel) testing contained approximately 800 test scripts, each consisting of a single test case; the current Level 2 testing consists of over 2,500 test scripts, each containing multiple test cases.

Approved chip readers are listed under "Level 1 Contact Approved Interface Modules" on the EMVCo website (www.emvco.com). IFM approvals are given for a four-year period from the time of testing. At the end of four years, a four-year extension, or "renewal" may be requested (typically by the vendor). The expiration date of the IFM approval is listed on the EMVCo website.

Approved EMV kernels are listed under "Level 2 Contact Approved Application Kernels" on the EMVCo website. EMV kernels are given an approval with a three-year expiration date, after which time a three-year renewal can be requested.

After the IFM or kernel has been tested, the testing laboratory will then forward the testing results to the EMVCo Secretariat. If all the tests have been passed, the Secretariat will issue a Letter of Approval (LOA) to the vendor. As noted, once the LOA has been issued, the IFM or kernel will also be listed on the EMVCo website.

The EMVCo administrative documentation notes that vendors can make "minor" changes to IFMs or kernels without invalidating the approvals. The documentation defines what makes a change "minor." Major changes will require that the updated IFM or kernel be tested against the current test suite.

IFMs or kernels that are being tested in order to extend a previous approval may fail one or more non-critical tests. In this case, a "restricted renewal" may be granted. The IFM or kernel will receive an LOA, but the restricted renewal is noted. At the time of this writing, payment networks with published rules in regards to EMV treat approvals and restricted renewals as equivalent.

An EMV approval is only an evaluation of an IFM's or kernel's adherence to the EMV specification. EMVCo has no say over suitability for deployment or for continuing presence in the field. Deployment and removal policies are determined by the respective payment networks, in consultation with ATM manufacturers and providers.

2.3 ICC Applications and Application Identifiers

The term "ICC (Integrated Circuit Card) Application" (commonly called the "card application" or "chip application") refers to a software application that resides on a chip card. Processing values and parameters that are associated with a particular application are stored in the chip. Although some parameters may be shared between multiple applications, many parameters have unique values for different applications. For example, the rules and parameters that govern a Maestro product are not the same as the rules and parameters that govern a Cirrus product. From the device standpoint, each application represents a unique product (normally with a distinct PAN).

Each ICC application is represented by an Application Identifier, or AID. Every AID is assigned by the ISO/IEC 7816-5 registration authority, and conforms 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.

The AIDs are usually referred to by their mnemonic. As an example, the AID "A00000002501"is associated with the mnemonic "American Express".

NOTE: ISO specifications may be found in the International Standards Organization website (www.iso.org). Typically, access to the specifications will require registration and a fee.

The chart below is a graphical representation of the relationship between the ISO/IEC specifications, the EMVCo specifications, some of the global payment network specifications (which are based on the EMVCo specifications), and some of the associated global payment network products, which have ICC applications.

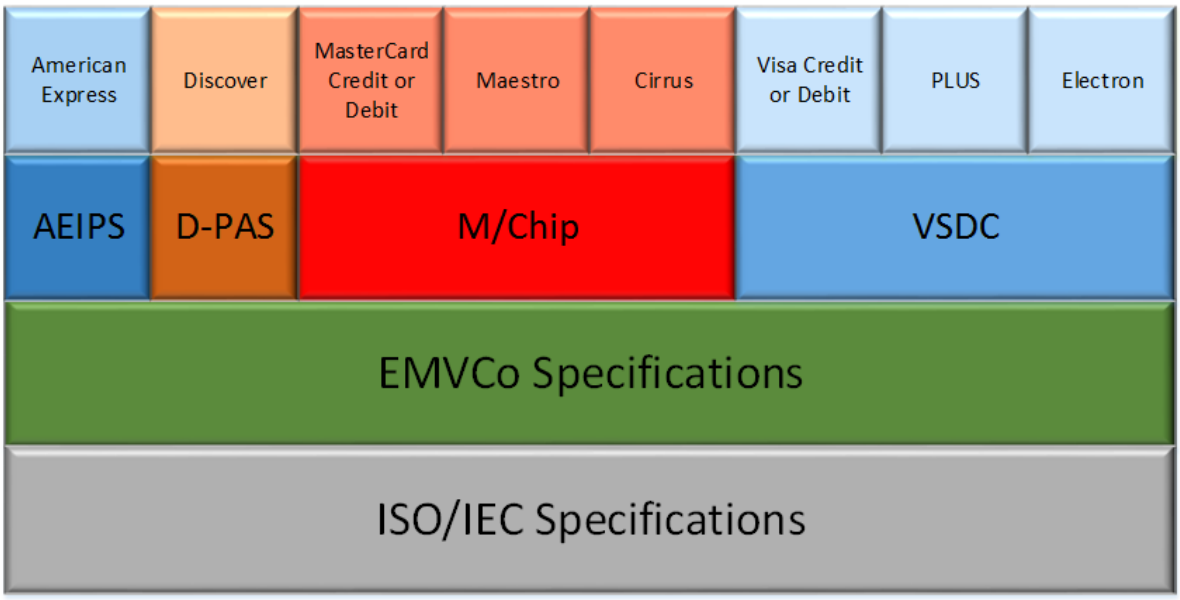

Diagram 2-2

Although the ATM most likely contains only one EMV kernel, the kernel can communicate with any chip application for which the ATM contains an AID. The RID of the AID is used to identify payment network specific processing decisions, embodied in parameters known as the Terminal Action Codes (TACs). Each payment network will define TACs to be associated with their RID. Further, each payment network may define processing and routing rules that apply to transactions initiated with an application (AID) associated with its network. For more information about the use of TACs, refer to Section 7.11.

2.4 Application Identifiers Used by Networks

The following chart shows a few of the most common ICC applications and their associated AIDs that are likely to be used at ATMs in the U.S. Some payment networks have more than one application (and therefore more than one AID) because they support multiple products, whereas other payment networks may only have a single AID.

Payment Network	RID	Product (Mnemonic)	PIX	AID
American Express	A000000025	American Express	01	A00000002501
Diners Club/Discover	A000000152	Discover	3010	A0000001523010
JCB	A000000065	Japan Credit Bureau	1010	A0000000651010
MasterCard	A000000004	MasterCard credit or debit	1010	A0000000041010
MasterCard	A000000004	Maestro (debit)	3060	A0000000043060
MasterCard	A000000004	Cirrus	6000	A0000000046000
Visa	A000000003	Visa credit or debit	1010	A0000000031010
Visa	A000000003	Visa Electron	2010	A0000000032010
Visa	A000000003	PLUS	8010	A0000000038010
U.S. Common Debit AID	A000000620	Common U.S. Debit AID – Debit Network Alliance (DNA)	0620	A0000006200620
U.S. Common Debit AID	A000000152	Common U.S Debit AID – Discover	4010	A0000001524010
U.S. Common Debit AID	A000000004	Common U.S. Debit AID – MasterCard Maestro	2203	A0000000042203
U.S. Common Debit AID	A000000098	Common U.S. Debit AID – Visa	0840	A0000000980840

Diagram 2-3

Non-U.S. networks may seek to gain acceptance in the U.S. through bilateral or reciprocal agreements with U.S. networks. These networks may use AIDs that are not on this list. ATM owners/operators wishing to accept those cards should obtain the necessary information from the partner U.S. networks.

Traditionally, a card issuer might have produced separate magnetic stripe cards for various purposes – for example, one card for a debit product, another card for a credit product. Chip card technology offers issuers the opportunity to place multiple products on a single chip, thereby eliminating the need for separate cards. So a chip card that conforms to EMV specifications will contain one or more financial applications, each identified by its own unique Application Identifier.

Some payment networks allow the issuer to extend the PIX to allow multiple iterations of a card application. For example, a Visa card might contain a credit application A000000003101010**1** and a debit application A000000003101010**2**. These numbers are assigned by the issuer, may not be sequential, and may differ from issuer to issuer. The application selection process, normally part of the EMV software provided by the ATM vendor or software developer, will need to account for this variability. For further discussion, see section 7.2 Application Selection.

Each chip-enabled payment device (ATM or POS terminal) will also support one or more financial applications, identified by Application Identifiers (AIDs). Through a process called Partial AID Selection, kernels can process all iterations of applications associated with each payment network's AID(s).

2.5 EMV Tags

An EMV data element is known as a "tag". The values involved in an EMV transaction (which reflect the issuer's implementation choices) are transported and identified by a tag which defines the meaning of the value, the format, and the length.

These tags may contain parameters established by the issuer, which are used during the interaction between the card and the terminal, or may be generated during EMV processing. They include information such as limits, counters, and actions to be taken for specific events, such as risk management. The values in these EMV tags can vary from one ICC application to another.

EMV tags use the BER-TLV encoding format, where BER stands for Basic Encoding Rules, and TLV stands for Tag Length Value. The Tag indicates the meaning or label, the Length identifies the number of bytes taken up by the Value, and the Value is the actual content of the data element. This concept is not unique to EMV; other industries use a similar construct. Sometimes the T will stand for Type instead of Tag in those other industries. Often, the BER-TLV format is referred to simply as the "TLV format."

Tags come in several formats. The value can be straightforward (as in the transaction amount), or encrypted, or padded with a leading or trailing character; or the value may represent a random number. Many EMV tag lengths and values use a technique called Binary Coded Decimal (BCD), where two characters represent one byte. In some cases the value of a tag is in hexadecimal, and must be converted to binary and each bit analyzed individually to interpret its meaning.

An example using BCD would be EMV Tag 9F02, which is the transaction amount. If the transaction amount is US$20.00, this tag would appear as 9F0206000000002000, where the Tag is 9F02 ("Transaction Amount"), the Length is 06, and the Value is 000000002000.

Some of the most common EMV tags that are used in an ATM transaction are described in Section 5.10.

The EMV specifications define a minimum set of tags that will be used or will be generated during EMV processing.[2] Some payment networks may have requirements for additional EMV tags to be used, or many even define payment network-specific tags for their products. However, with a few exceptions defined by individual payment networks, acquirers need not be concerned with specific tags, as their primary responsibility is simply to transport the tags to the payment networks. It is recommended that message formats include a flexible structure that allows for this transport. For example, message formats based on ISO/IEC 8583 can carry any number of EMV tags in the variable

[2] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 2, Section 8.1

field Data Element 55. Acquirers need not perform any manipulations to the EMV tags received from the ATM, but can simply transfer them from the ATM-to-acquirer message to the acquirer-to-payment-network message. By maintaining this flexibility, any newly defined BER-TLV format data can be transported with no impact to the acquirer, gateway, or transport network.

For more details about BER-TLV encoding, refer to the EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 3, Annexes A1, A2, and B.

For a comprehensive list of EMV tags as defined by EMVCo, refer to the EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 3, Annex A.

2.6 Application Preferred Name/Application Label

Each AID is personalized by the issuer to contain the Application Preferred Name, which is an identifier personalized by the issuer to be recognizable to the cardholder. This data is alphanumeric, with no special characters allowed except for “space”. As an example, an Application Preferred Name might be “ABC BANK DEBIT”.

The Application Preferred Name may or may not have the same value as the Application Label. Application Preferred Names are allowed to use a wider range of character sets than are used for Application Labels. The Application Preferred Name may even use a local or regional character set. Thus issuers may choose to personalize the Application Preferred Name in a format familiar to the cardholder. Application Labels are restricted to character sets in use by all EMV devices globally.

It is recommended that if the ATM supports the character set used for the Application Preferred Name, then the Application Preferred Name should be used for receipts and displays, otherwise the Application Label should be used. Following this recommendation is consistent with the recommendations and requirements of American Express, Discover, MasterCard, and Visa.

The EMV specifications state that when the Application Label or Preferred Name is displayed, the ATM must display all characters of the Application Label or Application Preferred Name. If the device is unable to display an invalid character, it must display a space instead.[3] The formats of the Application Label and Application Preferred Name allow spaces in these data elements. EMVCo notes that ATMs must not reject cards with spaces or invalid characters in these data elements.

For additional information about receipts, refer to Section 3.6.

[3] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 1, Section 12.2.4

2.7 Online and Offline PIN

When the PIN is to be authenticated online, the PIN is entered, encrypted, and transmitted to the issuer for verification. Although the EMV processing may indicate that an online PIN is to be used, the process of entering an online PIN for chip-initiated transactions is outside the scope of EMV processing. Thus the entry and authentication of the online PIN itself is not affected by the implementation of EMV. PIN security requirements continue to be set by the PCI Security Standards Council.

NOTE: *Chip acceptance devices should use the PAN received from the chip application and not the PAN encoded on the magnetic stripe when building PIN blocks, as some applications in a multi-application chip card may support a different PAN than that encoded on the magnetic stripe.*

The EMV specifications do support the functionality of "offline PIN", where the PIN is entered and verified against a reference PIN stored on the card's chip.[4] Currently, no U.S. payment network supports the use of offline PIN for ATM transactions. However, ATMs may be used for management of the offline PIN. A detailed discussion of offline PIN management is outside the scope of this document.

2.8 Service Codes

The service code is a three-digit code that is found in the Track 2 of the magnetic stripe. Per ISO/IEC 7813, the service code immediately follows the expiration date in the Track 2, as shown below.

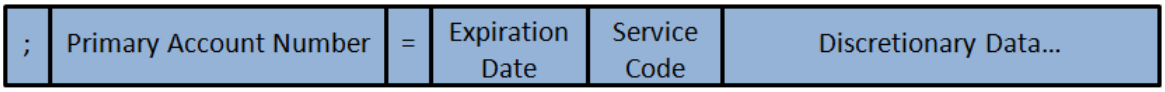

Diagram 2-4

The first byte of the service code is sometimes called the Alternative Technology Byte. Its purpose is to indicate whether the card was created as a magnetic stripe card or a chip card, and where the card can be used (i.e., interchange rules). Valid values are:

1: International interchange OK
2: International interchange, use ICC (Integrated Circuit Card; chip) where feasible
5: National interchange only except under bilateral agreement
6: National interchange only except under bilateral agreement, use ICC (chip) where feasible

[4] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 3, Section 10.5.1

7: No interchange except under bilateral agreement (closed loop)
9: Test

The first byte of the service code in magnetic stripe cards will contain a value of either 1 or 5; in chip cards (contact or dual interface) the value will be either 2 or 6.

There are other values in the service code relevant to magnetic stripe processing, which do not need to be considered for chip-initiated transactions.

While magnetic stripe-only cards are still predominant, the ATM may be configured to first read the magnetic stripe on the card, and interrogate the service code in Track 2 of the magnetic stripe to determine if the card is a chip card. If the service code begins with 1 or 5, processing will continue as it does today for a magnetic stripe card. If the service code begins with 2 or 6, the ATM will attempt to read the chip.

It is also possible to configure the ATM to try to read a chip before reading the magnetic stripe, which may be appropriate for ATMs that encounter a high percentage of chip cards.

The importance and use of the service code in an ATM transaction will be covered in subsequent sections of this document.

2.9 Issuer Scripts

Issuers can use the online transaction response as an opportunity to send a command to a chip card while it is in the field. The command is contained within an “issuer script” that is formatted by the authorization system and sent unaltered to the chip as part of the transaction response message. The chip will then attempt to execute the command within the script. The amount of information that can be sent in the script is limited by specifications and message size, so it is not possible to make major updates to a card, such as adding a new application, while the card is in the field; the card must be reissued for those types of changes.

Although both ATM and POS terminals can accept issuer scripts and pass them to a chip card, best practice in many regions of the world is for issuers to send scripts only with ATM transaction responses. It is very easy for a customer to remove a chip card from a POS device before the transaction response is received from the issuer; when this happens, if an issuer script were attached to the response, the script could not be passed to the card. With an ATM, the issuer has greater confidence that the card will be held by the ATM until the transaction is complete, so the script is very likely to be delivered to the chip card.

Common commands include application block and unblock, card block, PIN change, and PIN unblock.

However, not all payment networks support all of the scripts cited in the EMV specification, and the format of a particular script may vary slightly, depending on the card specification and application. Even if two payment networks both support a particular command, the networks may not use the

command in the same way. For example, MasterCard and Visa chip specifications both support the PUT DATA command, but they specify different fields that this command can update.

For more information on Issuer scripts, refer to:

- The EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 3, Sections 6.5 and 10.10
- The payment network chip card specifications.

2.9.1 Application Block

The Application Block command invalidates the application on the chip that is specified in the command. That application will no longer be eligible for selection by a terminal until it is unblocked. This is rarely done and would not be used for situations such as exhausted funds.

2.9.2 Application Unblock

The Application Unblock command reinstates the application on the chip that is specified in the command. That application is then eligible for selection by a terminal. Note that a special environment is required to deliver the Application Unblock command, such as an ATM specifically set up to perform this function.

2.9.3 Card Block

The Card Block command permanently disables all applications on the chip. None of the applications on the chip are then eligible for selection by a terminal. This action is final and cannot be undone.

2.9.4 PIN Change

PIN Change allows the issuer script to change the offline PIN stored in the card. PIN change considerations are outside the scope of this document.

2.9.5 PIN Unblock

The PIN Unblock script is supported by most chip specifications. This provides a way to “unlock” the offline PIN on the chip, typically when the PIN try counter has been exceeded. PIN Unblock considerations are outside the scope of this document.

2.10 Terminal Verification Results

The Terminal Verification Results (TVR – EMV Tag ‘95’) are a series of flags (bits) set by the terminal while processing a transaction initiated with a chip card. Some of the flags indicate:

- Offline data processing was not performed
- Offline data processing (SDA, DDA, CDA) failed

- Card number appears on hotlist
- Card and terminal have different application versions
- Expired application
- Requested service not allowed for card product (such as access to ATM cash disbursements)
- Cardholder verification was not successful
- PIN entry required, but no PIN pad present or not working
- Online PIN entered
- Transaction exceeds floor limit
- Issuer authentication failed
- Script processing failed

The TVR flags are evaluated during the different phases of Terminal Action Analysis to determine whether to terminate the transaction or to go online for authorization. EMV Tag 95 is typically sent to the issuer in an online transaction request; the issuer may use this information when making an authorization decision. See Section 7.11 Terminal Action Analysis for additional discussion.

3 Basic EMV Requirements for ATMs

This section addresses the hardware, software, and configuration required at the ATM in order to support EMV. For more details about project planning, refer to Section 4.

Each ATM vendor may have specific proprietary requirements, or support unique proprietary functionality. Each ATM owner/operator should communicate with their ATM provider(s) to understand any unique or proprietary aspects of a particular ATM make or model, as this may impact the EMV configuration for that equipment. Further, the ATM owner/operator should ensure that the ATM providers understand the business requirements of the owner/operator.

3.1 Card Reader

The ATM will need to be upgraded (or possibly replaced) to support a chip reader (InterFace Module [IFM]). It is the responsibility of the hardware vendor to obtain Level 1 approval from EMVCo. Refer to the hardware provider for questions about card reader hardware, durability, and other requirements. Chip readers typically have a comparable life span to magnetic stripe readers.

In contrast to many point-of-sale systems, ATM card readers support both chip reading and magnetic stripe reading with a single opening to insert or dip the card. Chip reading can be supported by motorized or dip readers. Swipe readers do not support EMV.

Because EMV processing includes several exchanges of data between the card and the ATM, the chip card must remain in the card reader for a period of time. This is in contrast to magnetic stripe processing where the data is simply read from the magnetic stripe.

3.1.1 Contact Styles

Currently available readers will use one of the following types of contacts:

Landing-style contacts

If no chip is detected during card insertion, the card is not moved to the chip station. If a chip is detected, the card is moved back into the chip reader, and the contacts drop, or "land" on the chip. This approach prolongs the life of the contacts by preventing damage from trying to "land" on non-chip cards and by reducing the amount of time the contacts are in physical connection with the card. Not all readers will have a sensor that can detect a chip; some may use a simple mechanical lever to land the contacts.

Friction-style contacts

The contacts float or roll across the face of the card, and end up in the correct position (on top of the chip) when the card stops moving. Friction-style contacts tend to wear out at a

quicker rate than landing-style contacts, largely due to the movement of the contacts across the card face on every card.

3.1.2 Motorized Reader

If an ATM has a motorized card reader, the chip reader component will need to be added. This component typically is attached internally to the end of the existing motorized card reader. When a card is inserted, the ATM may be configured to read the Track 2 first. If the service code in the Track 2 of the card begins with 1 or 5, the ATM retains the card in the front part of the motorized reader and proceeds with the transaction as a magnetic stripe transaction. If the service code begins with 2 or 6, the ATM pushes the card back into the chip reader component, which then attempts to communicate with the chip.

Advantages of using a motorized reader include:

- The cardholder will not be able to remove the card from the ATM before the transaction is complete; this significantly reduces the possibility of damage to the reader that can occur when the cardholder forcibly attempts to remove a card from the ATM. Motorized readers therefore may not have to be replaced as often as dip readers.
- The cardholder experience is very similar with a chip card as with a magnetic stripe card, in that the cardholder inserts the card, and the card is pulled into the ATM.
- The manner in which the ATM communicates with the card (i.e., magnetic stripe or chip) is invisible to the cardholder.
- It is possible for the ATM to retain the card and not return it to the cardholder.
- The internal motorized reader is generally better protected from the elements.
- Transaction chaining is available.

Disadvantages of using a motorized reader include:

- There is the potential for the cardholder to leave the ATM without taking the card. Refer to Section 6.3 for a discussion of “card before cash” vs. “cash before card”.
- There is the potential for a card to get stuck in the reader or inside the ATM, either through mechanical malfunctioning or due to devices inserted by criminals.
- Some financial institutions do not want to deal with cards that are stuck in, or deliberately retained by, the ATM; either the acquirer does not want to be responsible for foreign cards, or they do not want to go through the process whereby these cards are inventoried, then destroyed, or returned to the issuing institution.
- Motorized readers may be more costly to install and maintain.

3.1.3 Dip Reader

If the ATM has a dip reader, in order to ensure chip processing completes, it should include some type of cues to direct the behavior of the cardholder to leave the card in the reader. In addition to visual cues, it may be most effective for the dip reader to hold the chip card for the duration of the transaction. Some ATMs with dip readers will rely solely on visual cues to the cardholder to ensure the card is left in place. Dip readers may contain tactile cues, or even locking mechanisms to trap the card in place, but these may be most appropriate where a high percentage of cards are chip.

There are challenges when reading the magnetic stripe upon *insertion* into some dip readers; the magnetic stripe is therefore usually read when *withdrawing* the card from the dip reader. If the ATM interrogates the service code and determines that the card is a magnetic stripe card, the transaction can continue as it does today. However, if the card is a chip card, the ATM will prompt the cardholder to re-insert their card, and leave it in the reader for the duration of the transaction. This is sometimes known as the "double dip" scenario. One benefit of the "double dip" scenario is that there is no impact to magnetic stripe cardholders at the ATM; they still dip and remove their cards once. Only chip cards need to be re-inserted; messages on the ATM screen should instruct the cardholder to re-insert their chip card. ATM owners/operators should consult with the hardware vendor and software provider for assistance in configuring the "double dip" scenario.

Cardholder education will be essential to overcome the tendency to quickly remove cards. Proper signage and appropriate visual cues are strongly recommended.

Dip readers may use a pivot-style engagement to land the contacts onto the chip on the card. They "pivot" into contact position each time any card is fully inserted into the reader. There is less wear by using this "pivot" method than with friction-style contacts, but the mechanism does try to engage a chip on all cards. Contacts are released as the card is extracted, to eliminate any friction wear during extraction.

Advantages of using a dip reader include:

- It is less likely that the cardholder will leave without taking their card.
- It is less likely that the card will be stuck in the ATM.
- The ATM is unlikely to retain the card. (This is perceived as an advantage by many ATM deployers, issuers, and cardholders.)
- May be less costly than a motorized reader.

Disadvantages of using a dip reader include:

- The ATM is unlikely to retain the card. (This may be perceived as a disadvantage by some financial institutions.)
- The "double dip" scenario will be a change to cardholder behavior for customers with chip cards.

- The cardholder may forget to take their card at the end of the transaction, since they have been accustomed to removing the card in order for the transaction to proceed.
- Clear on-screen messaging and/or tactile or cues will need to be deployed to minimize disruption of chip transactions.
- Repair or replacement may be more costly or frequent due to exposure to the elements and the potential for damage by consumers.
- The fault rate may increase due to cardholders attempting to remove chip cards before the card reader has released them.

3.1.4 Contactless Reader

A few countries accept contactless cards at the ATM. Some regions have implemented contactless MSD (magnetic stripe data) whereas others have implemented contactless EMV. Some ATMs are capable of interacting with a mobile device, where a transaction can be pre-staged. Typically, the user will indicate at the ATM that they wish to initiate a contactless transaction; the ATM will not automatically select the contactless interface.

It is not clear at this time when, or if, U.S. ATMs will support contactless technology. Note however that support for mobile devices using NFC for payment is based on contactless technology in the acceptance device. ATM owners/operators will face a hardware upgrade whenever the decision is made to support contactless technology.

3.2 Operating System

For an EMV migration project, there are no specific operating system requirements. ATM owners should check with their hardware vendor or manufacturer to ensure that the operating system they are planning to use supports EMV and meets their specific technological and business needs.

Because support for Windows XP is ending, many Windows XP ATM owners (typically financial institutions [FIs]) are, or soon will be, migrating to Windows 7. This is a large project; ATM owners may therefore wish to consider the added complexity of simultaneously performing an operating system migration and an EMV migration project. Each ATM owner should balance the risks and dates associated with both projects, then determine the order in which they undertake these projects, based on their business needs.

Many non-FI ATMs use Windows CE as their operating system, which is not affected by the end of support for Windows XP. However it should be noted that lifecycle dates have also been announced for Windows CE releases. For example, Windows CE 5.0 has an Extended Support End Date of October 14, 2014. Deployers should check with their vendors to determine the impact, if any, of relevant Support End Dates.

For more information, refer to http://support.microsoft.com/lifecycle/.

Use of an "old" operating system does not mean that an organization will fall out of PCI compliance. However, as noted on the PCI SSC website, they must have compensating controls in place to mitigate for vulnerabilities that may exist when there are no further software updates for older operating systems. Compensating controls are a temporary solution until software can be upgraded to supported versions.

For more information, refer to https://www.pcisecuritystandards.org/faq/.

3.3 ATM Software

ATM deployers should check with their ATM software provider(s) to determine whether the EMV-capable ATM application software is compatible with the EMV-capable configuration that they plan to update or deploy. The ATM software itself is not subject to EMVCo testing or approval, although the card reader (InterFace Module, or IFM) and the kernel are tested by EMVCo laboratories.

3.4 EMV Software Kernel

Each ATM will require a tested and approved software component that implements EMV functionality, known as the EMV kernel. The kernel supports the command and response messages between the ATM and the chip, which are in a specific format called the APDU (Application Protocol Data Units) format, defined by EMVCo. The kernel also interfaces directly with the chip reader (IFM) and PIN pad. It is the responsibility of the kernel provider to obtain Level 2 approval from EMVCo for each kernel they provide. Although changes may be needed to the kernel when a new version of the EMV specification is issued, typically the EMV specifications are backwards compatible, and there is an extended time frame for kernels to be upgraded and approved under the updated specification. Refer to the EMVCo web site (www.emvco.com) and the ATM hardware/kernel provider for more information about kernel updates.

The kernel works in conjunction with the EMV application interface in the ATM. Each ATM owner should engage their ATM vendor to identify which payment networks they are affiliated with, and the brands of chip cards the ATM will need to accept. The ATM vendor will then be able to recommend the necessary software components. The vendor should be able to supply the payment network-specific parameters needed to support each brand; the kernel will use the parameters appropriate to each brand by examining the Registered Application Provider Identifier (RID).

The following diagram shows the relationship between the components of the ATM that are involved in an EMV transaction.

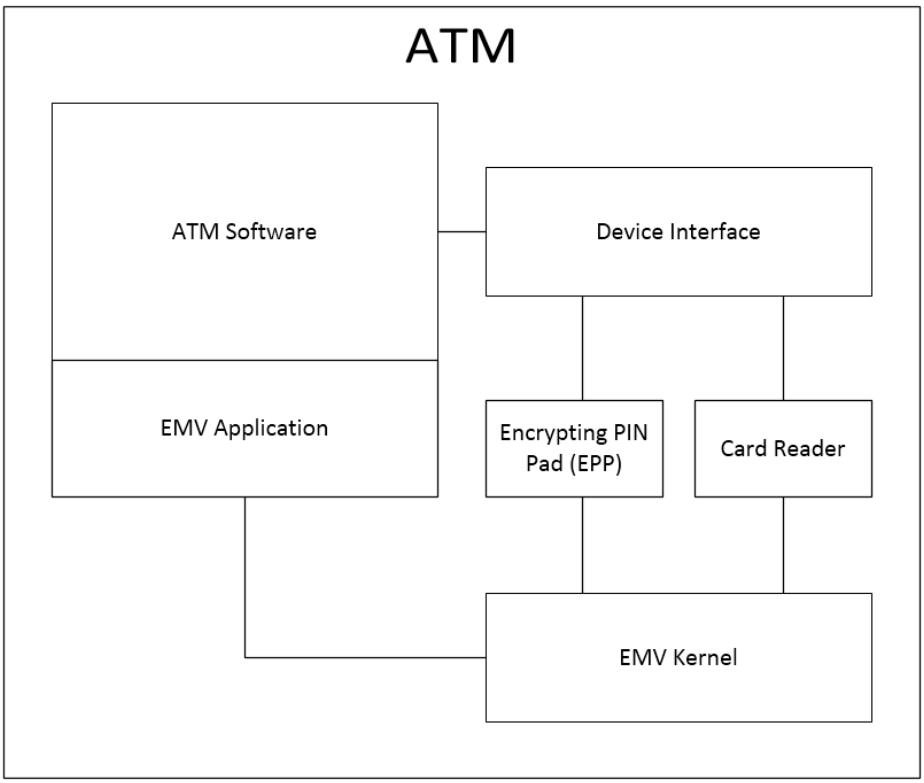

Diagram 3-1

With software that uses a legacy "states and screens" environment, it will be necessary to visit each ATM in person to install the EMV software kernel, since it cannot be pushed out to an ATM as part of a download when using this technology.

With some later technology, it is possible to push the entire image out to the ATM, and a site visit may not be needed in order to update the ATM software. When using a remote software delivery system, bandwidth, and the amount of time required for the download, may be a concern. Even when remote download is possible, ATM owners will still want to visit the ATM and test in person to ensure everything is functioning as expected after the download is complete.

ATM owners should discuss kernel deployment with their ATM vendors to determine what is needed for their specific environment.

3.5 Communications Protocol

The communications protocol (e.g., frame, wireless, dial-up) that is used by the ATM to communicate with the host/switch will need to support the longer EMV messages. Ideally, it will maintain sufficient speed (time to complete a transaction) and data integrity to ensure a satisfactory customer experience.

3.6 Receipts

EMVCo mandates that the Application Identifier (AID) must be printed (in hexadecimal characters) on all receipts for EMV transactions[5]. This will require a change to the ATM's receipt file. However, the AID value alone will be meaningless to the customer. EMV specifications allow the ATM owner to include additional information if desired.

If the ATM screen and the ATM printer support the Issuer Code Table Index, the ATM should display and print the Application Preferred Name of the application used to initiate the transaction. If the ATM screen or the ATM printer does not support the Issuer Code Table Index of the Application Preferred Name, the Application Label should be displayed and printed on the receipt. It is important that either the Application Preferred Name or Application Label is consistently used for both the screen and the receipt. Although the individual payment network requirements may be worded slightly different from what is stated above, this recommendation is consistent with the known recommendations and requirements of American Express, Discover, MasterCard and Visa.

For multi-application cards, it is important to display on the screen, and print on the receipt, the Application used. The Application Label or Application Preferred Name can be displayed at any appropriate time in the transaction processing; Account Selection or PIN entry are often useful points to display the Application Preferred Name/Application Label.

3.7 Configuration

The ATM configuration will need to be modified to incorporate the following. If remote downloads are supported, determine whether support for these items should be included in the download process.

- List of supported Application Identifiers (AIDs); e.g., Cirrus, Maestro, PLUS
    - In order to process transactions as chip, the ATM must contain a list of the supported AIDs for all payment networks supported by the ATM (refer to Section 2.3 for more details).
- List of EMV Tags that will be sent to the acquiring system
    - Ensure that the ATM reads or generates all tags required by the payment networks that are supported by the ATM, and includes those in the message to the ATM-driving host.
- Set the value for Terminal Action Codes (TAC)
    - Ensure that the TACs specified for each payment network supported by the ATM are properly set. Each AID will have an associated set of TACs as specified by those

[5] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 4, Section 11.4

payment networks. In today's environment, the TACs supplied for ATMs will indicate that all transactions are to be sent online. (Refer to Section 7.11 for more details.)

The following items are normally only configured once:

- Terminal floor limit
  - In today's environment, will be set to zero for ATM transactions (all transactions will go online)
- Cardholder Verification Method (CVM)
  - In today's environment, will be set to online PIN, as ATMs do not support other CVMs at this time. Refer to Section 7.7 for more information about the CVM.
- EMV-specific fields stored in the ATM
  - For example, Application Selection Indicator, or ASI (refer to Section 7.2 for more details)
- Supported languages and currencies
  - Review these items to determine that if/when the ATM supports multiple languages or currencies, it either provides a choice to the cardholder or recognizes the preference specified in the chip. (See Section 7.4 for more details.)
- EMV Enablement (turn EMV on) once all configuration, testing , and certification are complete

The following items are implementation considerations:

- Issuer scripts
  - As required by EMV[6], the ATM must be able to pass scripts from the issuer to the chip if the issuer sends scripts as part of a transaction response. (The card will pass a flag indicating completion status of script processing as part of the next online transaction that is performed; this information will be forwarded to the issuer as part of normal EMV processing.) Note that this is a fundamental function of EMV and cannot be turned off. This is a factor in the consideration that the card not be removed from the station until all EMV processing is complete. This will normally be "built in" to the ATM and likely not something the ATM deployer or processor will have to configure.
- New screen messages to cardholders
  - It may be necessary to add messages such as a "Please Wait, Transaction Processing" while the terminal and the chip are exchanging information, so that the cardholder realizes that the transaction is indeed proceeding and they do not attempt to cancel the transaction or remove the card prematurely. Care should be

[6] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 3, Section 10.10

taken to display messages that make sense to the cardholder and are not overly technical. For example, a message stating "no matching AID could be found" would be meaningless to a cardholder. Remember to modify any voice guidance (e.g., .wav files) to include new messages.

- State and screen flow (legacy ATM environments)
    - Refer to the appropriate vendor (e.g., manufacturer, software provider, processor) documentation to implement new states and screens that are required for EMV.

Normally, the ATM will provide all functionality to chip cards as is provided to magnetic stripe cards.

For more information about the required configuration, refer to the relevant ATM software documentation provided by the ATM vendor.

3.8 Encryption Keys

Existing encryption keys at the ATM are sufficient for EMV; no new keys are required at the ATM to support EMV.

Public keys and Public Key Infrastructure (PKI) are used for offline functions, such as Offline Data Authentication and Offline PIN Verification. Since these offline functions are not used at ATMs, there is no need to set up a public key management system to support ATM acquiring.

The PIN will be encrypted by the PIN pad in the same way for both magnetic stripe and EMV transactions. Functions such as Remote Key Loading are outside of EMV.

3.9 Testing and Approvals

Terminal vendors will need to obtain the following EMV approvals for devices:

- Level 1: InterFace Module (IFM)/chip reader functions
- Level 2: terminal software application functions (EMV software kernel)

Although chip reader and kernel approvals are normally obtained by the vendor, each ATM owner and/or ATM licensee should verify that the chip readers and EMV software kernels they select have only passed these two testing processes. Preferably the chip reader and kernel are already in use elsewhere, if possible, as when using a newly-created kernel and/or IFM model, additional testing will likely be needed. Normally, each ATM configuration (combination of chip reader, EMV software kernel, and acquirer-to-ATM message format) will need pre-deployment testing.

In addition to these approvals, each ATM processor will need to pass the certifications mandated by the payment networks with which they are associated. For more information, refer to Section 4.3.

As noted, normally the ATM vendors will obtain the chip reader and EMV kernel approvals. However, the ATM deployer should check with the vendor to ensure the approvals were obtained and are current.

While pre-deployment tests are required for each configuration, some vendors and/or acquiring processors may offer “pre-tested” configurations. The ATM deployer should check with their ATM vendor and with their ATM processor to ensure all required tests have been performed. If the deployer has ordered a customized configuration, they may need to arrange for testing to be performed on that customized configuration (usually by the party performing the customization).

4 Migration Planning

4.1 General Considerations

When should ATMs migrate to EMV? Each ATM owner/operator will need to make their own business decision, based on factors such as the cost of migration, liability shift dates, their tolerance for risk, and other projects currently on their plate (such as Windows 7 migration). Some ATM owners may decide not to upgrade a particular ATM to EMV until they must replace the ATM (according to their regular replacement cycle) or until they have to replace a broken card reader. **If an ATM needs to be replaced before EMV migration begins, the owner/operator may wish to consider including a chip reader (IFM) as part of the replacement; it is much less costly to include the chip reader when purchasing the ATM than installing it later.**

EMV migration can be a 9-12 month project (or longer), from inception to implementing the first EMV-enabled ATM in the field. There will probably be some prerequisites before beginning the project; these can vary depending on whether the ATM operator drives their own ATMs, goes through a processor, and other factors. ATM owners/operators should confer with their ATM manufacturer(s) and processor(s) before embarking upon the migration process.

"When to migrate to EMV" is an individual ATM owner's decision. When an ATM owner does decide to migrate to EMV, the effort may initially seem overwhelming. But as with any other major project, thorough planning, communication, and coordination are the keys to success. ATM owners/operators are encouraged to:

- Read this white paper to get an idea of what will be involved in the project
- Formulate business requirements, to include:
    - Which cards will be acquired
    - Which networks are supported
    - Which transactions will be supported
    - Anticipated transaction paths
- Create a Business Requirements Document and/or Project Charter
- Consult with hardware/software vendors, processors, and payment network representatives for their recommendations and advice
- Work closely with vendor(s) during the implementation process
    - Verify that components have passed EMVCo Level 1 and Level 2 approval testing
    - Verify that the vendor has a software kernel that meets business requirements
    - Verify that the processor has completed and secured all the required testing and certifications for their platform and all applicable end-to-end configurations
    - Rely on the vendor to help with the technical details of EMV, and obtain the EMV-compliant hardware, software, and processing components
- Coordinate project activities with payment network representative(s)

To help ensure a positive customer experience, the ATM EMV migration project team within a financial institution is encouraged to review their plans with the card-issuing side of the organization. A financial institution may wish to coordinate chip card issuance with ATM upgrades, so that cardholders have convenient locations to use their new chip cards. If timeframes do not initially align, the ATM project may choose to upgrade ATMs to support EMV, but not "turn EMV on" in those ATMs until a certain number of chip cards are in production, bearing in mind the potential risk for "not-on-us" of this decision based on the liability shifts.

For ATM deployers that are not part of an entity that issues cards, such as a non-branded independent sales organization (ISO), the market should be monitored to get a sense of what others are doing, to determine when migrating will be most helpful. ATM processors may be able to provide reporting on the number of chip cards being presented at the deployer's ATMs so that the potential liability can be assessed prior to the liability shift date. ISOs should work with their branding partner and/or ATM processor to determine their partner's EMV compliance plans.

4.2 Upgrade or Replace

In order to understand the scope of their EMV implementation, each ATM owner will need to undertake a detailed inventory of their current ATM fleet. Begin by determining the makes (e.g., Diebold, NCR, Triton, Hyosung, Genmega, Wincor Nixdorf) and models of ATMs, and the firmware/software in use on those ATMs.

Because upgrades are typically less expensive than wholesale replacement, ATM owners will want to identify any terminals that can be made EMV compliant. These are terminals for which equipment (such as chip readers) and software upgrades are available to ensure that the terminal meets the security, interoperability, and functionality requirements outlined by EMVCo. Ensure that the project schedule allows time for budget approval, and for ordering and installing the required new parts or devices.

Some ATMs may be old enough that EMV-related parts cannot be obtained, or the cost of those parts is prohibitive. These ATMs will need to be replaced with models that can support EMV. When replacing an ATM, physical changes may be needed to the surrounding area. For example, replacing through-the-wall ATMs may mean remodeling at the branch in order to accommodate terminals with different dimensions. These changes can have a substantial impact on a project timeline and budget.

Because EMV implementation is so far-reaching, it offers an opportunity for acquirers (especially those that have acquired other institution's ATM networks via mergers) to re-evaluate the supported types of ATMs (manufacturers and models), and the number and location of ATMs in the network. For every unique ATM type supported, there are direct costs (e.g., equipment purchase price, third-party service agreements, vendor maintenance agreements, certifications) as well as associated costs (e.g., a test lab with representative terminals, in-house expertise, development that is specific to each terminal make and model). When evaluating these costs, institutions may

determine that the cost of replacing some terminals is offset by the savings realized by supporting fewer terminal types. For example, acquiring more devices from a single vendor may result in more favorable terms in a service contract. Fewer unique combinations of terminal make, chip reader, and software kernel will also result in fewer costly testing cycles, as each payment network may have their own testing requirements..

4.3 Certification, Testing, and Approvals Needed

As noted in Section 3.9, EMVCo issues Letters of Approval for various hardware and software components, and lists approved products on www.emvco.com. Currently, American Express, Discover, MasterCard and Visa require that ATMs accepting chip cards must have an:

- EMV Level 1 Approved Card Reader ("IFM" or "hardware")
- EMV Level 2 Approved Application Kernel ("software")

Upon completion of EMV testing, the ATM provider (the ATM hardware vendor for the chip reader, and either the ATM provider or a third-party software provider for the kernel) will receive a Letter of Approval (LOA) from EMVCo for each tested product. These ATM providers should be able to present these letters upon demand. Alternatively, the EMVCo website (www.emvco.com) can be searched for approved products, though in any case this often requires the appropriate kernel and IFM identifiers as determined by the ATM providers.

ATM owners need to be aware that they will be responsible for multiple levels of certifications. This topic is covered in great detail in the EMV Migration Forum white paper, "EMV Testing and Certification White Paper: Current U.S. Payment Brand Requirements for the Acquiring Community," available at this link:

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

It is also important to note that the certifications required by the relevant payment networks are designed to test functionality that is important to those networks, and ensure that EMV data is handled correctly by the terminal and the network as per the network's specification. These certifications will not cover all types of testing that an ATM owner, acquirer, or issuer will need to perform. Regression testing, new feature testing, specific EMV testing, performance testing, volume testing, and stress testing may be needed prior to certifying with a payment network. It is vital to test the exact ATM configuration and software that will be used in production; therefore, internal testing should be completed prior to initiating formal certification with the networks. As noted previously, it is very likely that ATM vendors have already obtained all EMV approvals, and that the network certifications will be completed by the ATM processor. Further, either the vendor or processor may offer "pre-tested" configurations that will remove the burden of testing from the individual ATM deployer. ATM deployers may wish to specifically seek out "pre-tested" configurations to avoid pre-deployment testing. (It is recommended that some basic regression testing be performed at each new or updated EMV-capable ATM.)

4.4 Migration Planning Tasks

Although every ATM owner's EMV migration project will have its own particular challenges, the following steps will be common to most, if not all, ATM owners.

4.4.1 Hardware and Software Evaluation

- Evaluate existing ATM hardware
    - Determine if there are any ATMs that cannot be upgraded for chip
- Determine which EMV-approved upgrade packages (or complete ATMs) are applicable/available
- For new or customized configurations, obtain EMV approvals (if new or customized configurations do not implement currently approved IFMs and kernels)
        - Ensure custom vendor meets current EMV standards, as well as the standards of the payment networks in which the ATM participates
        - Ensure custom vendor contacts the appropriate EMVCo-certified testing laboratory
        - Ensure that the custom vendor obtains approval for EMV Levels 1 (IFM) and 2 (kernel)
        - Negotiate product time frames for delivery
    - Select hardware upgrades or replacements
- Evaluate existing ATM software
    - Determine which EMV-approved software packages are applicable/available
    - Evaluate software customization/integration requirements
    - Finalize requirements and negotiate required modifications and ongoing service
- Evaluate hardware and software maintenance options
    - In-house
    - Third-party
    - Negotiate contracts with suppliers
- Develop ATM chip migration strategy, including plans for ATM replacement or upgrade. Note that even if the ATM is EMV-hardware ready, the size of the software update will be quite large and may necessitate a site visit even if remote download functionality is available.

4.4.2 Policy and Requirements Definition

- Make policy decisions related to EMV ATM requirements
    - Obtain chip requirements and recommendations for ATMs from the payment network representative
    - Determine which card brands will need to be supported and implement the appropriate Application Identifiers (AIDs) to support those brands (see section 2.4)
        - International card programs
        - Domestic schemes
        - Define requirements for the application selection method(s) selected
            - The EMF recommends that cardholder selection be implemented for multi-product cards
            - Customized selection may be needed to preferentially select a Common AID over its linked international AID(s)
    - Decide which languages ATMs will display
        - National language(s)
        - International languages for high volumes of customers
    - Decide whether to implement cardholder selection/confirmation
        - This may already be determined by the EMV software provided by the ATM manufacturer
    - Configure Terminal Action Analysis
        - Obtain the set of TACs that are applicable to the ATM from the payment network representative (see also section 7.11)
    - Check with the payment network representative to understand their transaction-type requirements related to reversals, balance inquiries, funds transfer, and deposits
    - Work with the payment network representatives to understand their fallback policies
    - Define any proprietary ATM requirements
    - Make any policy decisions required to implement other ATM requirements
    - Determine if PIN Change/PIN Unblock is desirable and whether it is available from the payment networks used
    - Determine additional applications to be processed or supported by the ATMs, such as loyalty or stored value
    - Work with the ATM vendor to ensure that the devices read chip cards via the chip reader (IFM)
    - Define impacts to online transaction processing systems
    - Define impacts to clearing and settlement
    - For ATM deployers associated with an issuance division, review potential impacts to the customer experience with the card issuance division to ensure all areas

understand “what will happen with my card at my ATM”

4.4.3 Review User Experience

- Ensure the ATM’s user interface prompts cardholders through the new experience
    - Consider placing an icon on the card reader both to indicate chip-readiness and to demonstrate the correct orientation when inserting the chip card (EMVCo offers graphic files for such icons. Search www.emvco.com for “Terminal Icon”.)
    - For dip readers, consider implementing messaging to support “double dip” (see section 1.1.1 and section 6.3)
    - In addition to on-screen messaging, consider adding a placard instructing cardholders to leave the card in the dip reader until instructed to remove the card.

4.4.4 Implementation

- Complete all operations activities required to comply with market requirements
    - Work with vendors and technical staff to implement the appropriate configuration, including:
        - The recommended cardholder selection processing for the market
        - Processing Restrictions
        - Terminal Action Codes
- Complete all activities required to implement other ATM requirements
    - Interface with technical staff to ensure support for proprietary processing
- Update documentation and training manuals
    - Document available languages in operations and training manuals
    - Include the TACs in documentation for operations and service staff
    - Outline the additional applications, such as loyalty or stored value, in operations manuals
- Define strategy for:
    - Production roll-out
    - Training of internal staff (e.g., customer-facing personnel such as branch staff, technical support)
    - Internal and external communication

4.4.5 Certification

- Communicate business requirements to vendors and payment network representatives
- Become familiar with the required certifications, which may include a “Beta Test” post-implementation
- Obtain the tools and documentation (e.g., certification test plans) required for certification
- Schedule certification test windows
- Perform in-house pre-certification to work out issues before attempting formal certification

4.4.6 Additional Considerations

A minimum of six to nine months should be allowed to develop and gain approval for a new device. It is recommended that ATM providers contact the applicable certification authority well in advance for estimated approval timing.

It is recommended that ATM providers choose chip readers that have been tested and approved recently, as EMV testing is regularly updated to reduce occurrences of interoperability problems.

Upgrading, replacing, or adding a card reader in an ATM will require a site visit. The ATM owner may want to combine this with the installation of the EMV software kernel(s).

The ATM deployer should also determine if the ATM provider has identified operational considerations for EMV deployment, such as power supply and grounding specifications.

5 General Considerations

5.1 Routing

The Application Identifier (AID) that is selected by the terminal is not used to route a transaction by any acquirer or network in the world today. In the U.S., as in many other countries, the routing path for an online transaction request (including EMV requests) is typically determined based on the BIN/card prefix, and, in some cases, in conjunction with applicable interchange agreements and/or fees.

There is no EMV processing that inherently assumes that any given transaction will be routed over a particular network. However, at the time of this writing, MasterCard and Visa both require that transactions initiated with their respective global AIDs be routed to a network associated with the affiliated brand. Transactions initiated with a Common Debit AID can be routed using current arrangements (i.e., BIN routing tables).

All information that directs processing of the transaction is carried in the message itself. All networks must pass a minimum set of EMV Tags (as defined in the EMV specifications[7]), with their values unaltered and in their original form, to the issuer or issuer's processing agent, regardless of the transaction path that is selected; the EMV data can be used when authorizing the transaction. Although each message format may carry the EMV data in different fields, or present the fields in a different order within a message, all network specifications will adhere to EMVCo standards regarding the minimum number and type of data fields that must be included in the transaction request message. A key challenge is ensuring that, regardless of the selected transaction path, the issuer or issuing processing party receives all the data it needs to properly authenticate the chip card, verify the cardholder, and authorize the transaction. The cryptogram version number and the Derivation Key Index (DKI) of the TDES key are carried in the online request message so that the issuer may validate the cryptogram regardless of the network used to transport the transaction.

Because all ATM transactions go online to some form of a host system for authorization, and the only cardholder verification method that is supported at the ATM is online PIN, both the application cryptogram (the ARQC) and the encrypted PIN will be passed by all networks that support EMV-based ATM transactions.

Although it is certainly technically possible to route by AID, most acquirers, processors, and networks have complex routing logic in place today which would have to be significantly modified to take the AID into consideration when routing. One of the primary goals of U.S. payments industry

[7] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 2, Section 8.1.1

stakeholders is that the implementation of EMV in the U.S. will not impact routing that is in place pre-EMV.

5.2 Liability Shift

Three of the four global payment networks (Discover, MasterCard, and Visa) have published liability shift dates that impact ATM owners. The intent of these shifts is to assign liability for counterfeit card fraud to the party in the transaction that is using the less secure technology (magnetic stripe).

These liability shifts are not mandates; therefore ATM providers and acquirers are not absolutely required to migrate to EMV. However, the liability shift provides a strong incentive to do so. In the case of an independent ATM provider, the liability threat from even a small amount of fraud exposure could well compromise the viability of that provider.

In the current magnetic stripe environment, when a transaction is determined to be the result of counterfeit card fraud, the burden of the fraud loss typically falls upon the issuer. ATM owners and acquirers have historically not had to bear the liability for this type of fraud loss, because it was not within their ability to materially address such fraud.

With the liability shift, the party in the transaction that does not support EMV transaction processing and therefore supports less secure technology (i.e., magnetic stripe) will bear the fraud loss. Here are some sample transaction scenarios.

Terminal Technology	**Card Technology**	**Transaction**	**Responsible Party in the Event of Counterfeit Card Fraud**
Magnetic stripe only	Magnetic stripe only	Magnetic stripe	Current practice (business as usual); liability shift does not apply post-liability shift dates
Magnetic stripe only (not EMV compliant)	EMV/chip and magnetic stripe	Magnetic stripe	ATM owner would be responsible for any loss due to counterfeit card fraud
Certified EMV/chip compliant	Magnetic stripe only	Magnetic stripe	Issuer would be responsible for any loss due to counterfeit card fraud
Certified EMV/chip compliant	EMV/chip and magnetic stripe	Fallback to magnetic stripe (chip was not read)	Refer to rules from governing payment network

Diagram 5-1

- Any time the chip is successfully read, it is expected that the issuer will verify the ARQC and interrogate additional EMV data in the transaction. If the issuer approves the transaction without validating the ARQC or if the ARQC could not be validated, then the issuer will likely be liable for the fraud loss.

Interested parties should contact their payment network representative for each of the networks they participate in to obtain current information about liability shifts for each payment network, including dates and policies.

5.3 Transaction Log

Some ATMs maintain transaction logs to support research and trouble-shooting. Check with the terminal provider to determine logging functionality (e.g., what type of logging is supported, how long data can be maintained). If the ATM is able to store transaction data, it is recommended that the device transaction log contain the following items:

- Transaction amount indicated in transaction currency
- Account number (at least four digits can be truncated or masked)
- Type of account accessed
- Transaction date
- Authorization code
- Transaction type (cash disbursement, balance inquiry)
- AID of application selected, with suffix (if present) *[new with EMV]*
- Terminal Verification Results (TVR) *[new with EMV]*
- Card Verification Results (CVR) *[new with EMV]*
- Transaction Certificate (TC) *[new with EMV]*

This information will help with problem resolution. Also, if a decline occurs, it will help with customer service.

5.4 Encrypting Pin Pad Requirements

Currently, a number of payment networks require the Encrypting PIN Pad (EPP) to meet PCI security requirements. As indicated in Section 3.8, there are no new requirements for the PIN pad in order to support EMV, so existing ATM PIN pads will continue to work as they do today.

5.5 Exception Conditions

ATM processing exceptions, such as dispense failure or time out, will be processed in the same way for chip transactions and magnetic stripe transactions. In most cases, a reversal message will be sent; there are no EMV considerations for the reversal message itself. For exceptions occurring during processing, the transaction either will be terminated or restarted (contacts de-energized, with new reset for restarts).

If the reversal occurs because the chip card declined an approved transaction due to issuer authentication failure, the Terminal Verification Results (TVR; EMV Tag 95) and the Issuer Application Data (IAD; EMV Tag 9F10), as returned from the card in response to the second

Generate Application Cryptogram, may provide useful information if included in the reversal message. If available, Issuer Script Results (tag 9F5B) can also be sent. Individual payment network specifications should be consulted to determine what chip results are to be included in the reversal message.

For system-generated reversals and other reversals where the updated TVR/Issuer Application Data values and Issuer Script Results are not available, the TVR/Issuer Application Data and the Issuer Script results do not need to be provided.

5.6 Card Data in Online Message

To support correct EMV processing, the ATM should ensure that if a transaction is initiated using the chip (i.e., the chip on a chip card was successfully read), all transaction data used in the authorization message, including the Track 2 Equivalent Data, is read from the chip, or is the result of EMV processing. Correspondingly, if a transaction is initiated via magnetic stripe (including fallback transactions), any data elements, including the track data, used in the transaction should be read only from the magnetic stripe, to ensure that the authorizing entity has the appropriate data to perform functions such as CVV verification.

Note that in many cases, for security reasons, the track data carried on the chip differs slightly from the track data on the magnetic stripe. When authorization is being performed, the card issuer may consider whether the track data sent actually matches the identified initiation mode (i.e., chip vs. magnetic stripe) as part of the risk analysis.

Note that for a multi-product card, the track data in the selected chip application may not match the physical magnetic stripe data at all, as the physical magnetic stripe data may be tied to a product that was not selected. For this reason, once a transaction is initiated using the chip, any data read from the magnetic stripe should be discarded and should not be considered in any processing.

5.7 Transaction Chaining

ATMs often support Transaction Chaining, where a transaction is completed by offering another service. In this way, cardholders can complete several transactions without retrieving and re-inserting their cards.

The important considerations for Transaction Chaining are:

- During an EMV session (Cash Disbursement), following contact activation[8], the first thing that is done is Application Selection to build the candidate list (see section 7.2).

[8] Energizing of the contacts

Some sample scenarios of Transaction Chaining are outlined below:

1. Single application card – Balance Inquiry followed by Cash Disbursement (Non-cash[9] transaction using EMV functions followed by EMV transaction) {User response in braces}
   Insert card
   Activate <<ATR>>
   Application Selection to build candidate list
   {only one matching application found}
   Select application (automatically, or by cardholder)
   Prompt for PIN {PIN}
   Transaction Selection {Balance Inquiry}[10]
   Account Selection {Checking}
   Perform balance inquiry (using EMV functionality)
   Ask cardholder if additional transaction {Yes}
   Select application
   Transaction Selection {Withdrawal}
   Account Selection {Checking}
   Perform cash withdrawal [Using PIN entered earlier since same application]
   Ask cardholder if additional Transaction {No}
   Deactivate
2. Multi-application[11] card – Balance Inquiry followed by Cash Disbursement (Non-cash transaction using EMV functions followed by EMV transaction)
   Insert card
   Activate <<ATR>>
   Application Selection to build candidate list
   Cardholder Selection {XYZ Debit}
   Select application
   Prompt for PIN {PIN}
   Transaction Selection {Balance Inquiry}
   Account Selection {Checking}
   Perform balance enquiry

[9] See "Other ATM Transaction Types"

[10] In any case where Cardholder Selection was not performed, it is recommended that the Application Label or the Application Preferred Name (if character set supported by ATM) be displayed on either the Transaction Selection or Account Selection screen.

[11] This refers to a true multi-product card, ("combo" or "combi" card), where more than one application will be presented to the cardholder for choice. Cards containing both a Common Debit AID and a linked, branded AID are most likely a single product (debit) card, with a single application supporting the two AIDs.

Ask cardholder if additional transaction {Yes}
Ask cardholder if same application {Yes}
Select application [Same application as used before]
Transaction Selection {Withdrawal}
Account Selection {Checking}
Perform cash withdrawal [Using PIN entered earlier since same application]
Ask cardholder if additional Transaction {No}
Deactivate

5.8 Service Level Agreements

ATM owners frequently ask if an EMV transaction will "take longer" than a magnetic stripe transaction.

The interaction between the chip card and the terminal does take longer than a simple read of a magnetic stripe, but this interaction is typically very fast; seconds rather than minutes. Some ATM owners display a "please wait, transaction processing" message to the cardholder while this interaction is occurring, so that the cardholder understands that the transaction is proceeding and they do not attempt to cancel the transaction or remove the card prematurely.

The maximum amount of time allowed for a transaction, which may be included in a Service Level Agreement (SLA), usually starts when the transaction request leaves the terminal and ends when the response reaches the terminal. This would not include the time required for the card-terminal interaction, which occurs before the transaction request leaves the terminal.

Additional steps are required by the issuer during the transaction authorization process, such as verifying and generating cryptograms, and checking other EMV data in the transaction request. Experience in other regions has shown that these steps do not add enough time to transaction processing to be a concern.

5.9 ATM Non-Cash Transaction Types[12]

Some issuers may question the need to perform EMV processing, including sending the ARQC, in a non-financial transaction such as a mini-statement print. However, ARQC generation is a standard part of EMV functioning. Most cards do not evaluate the transaction code, or even the environment (terminal type), so they may not even distinguish between POS and ATM, let alone transaction type.

[12] The discussion throughout this section is based on "*Recommendations for EMV Processing for Industry-Specific Transaction Types"* which can be downloaded from the EMVCo website (www.emvco.com).

Therefore, a chip card will always generate a cryptogram (an ARQC or an Application Authentication Cryptogram, AAC), and if an ARQC is generated, the ATM will send it to the issuer for authentication/verification. If the issuer wants to ignore the ARQC (and some do), that is their prerogative, although they need to be aware that by doing so, they are negating the biggest benefit of EMV. Some issuers simply use the Track 2 Equivalent Data from the chip (which is not exactly the same as the Track 2 data in the magnetic stripe) to prove that the transaction was initiated by the chip card.

Besides Cash Withdrawals (also known as Cash Disbursements or Cash Advancements), ATMs typically support other financial management transactions, such as Balance Inquiry. Although these are not considered "EMV transactions[13]", EMV-defined steps (in italics; see Section 7 for more information on any of these steps), can be used to initiate these transaction types, such as *Application Selection, Initiate Application Processing,* and *Read Application Data*. To support the current known requirements of payment networks, the CVM (see Section 7.7) should continue to be Online PIN[14]. The issuer likely will validate the transaction initiated at the ATM using *Card Authentication Method* as part of online processing. For these transactions, the device would not use the EMV-defined *Terminal Risk Management* or *Terminal Action Analysis. Completion* will always consist of generating an AAC, to ensure that counters are not improperly reset.

Special transactions can be implemented specifically to support *Issuer-to-Card Script Processing*, such as PIN Change.[15]

Reading of information or requests for identification or authentication can be done using EMV functions. To ensure proper controls remain in place, functions that would affect risk management or update counters should not be executed, except by defined EMV transactions (Cash Withdrawal)[16].

Acquirers who wish to use EMV functions for non-EMV transactions should discuss these requirements with their vendors. Vendors may include many of the non-EMV transaction types listed here as part of their base offering, but may not offer direct access to EMV functions. This can make it difficult to develop proprietary functions in the future.

[13] *Core* EMV transactions involve dispensing of cash *or* sales of goods or services.

[14] Individual payment networks may announce support for new CVMs in the future.

[15] PIN Change/Unblock may use some of these functions. PIN Change/Unblock is only implemented in a few markets.

[16] The Get Processing Options command in *Initiate Application Processing* will update the Application Transaction Counter (ATC).

5.9.1 Balance Inquiry

ATM Balance Inquiry allows a cardholder to determine the available balance for the account(s) associated with the card. When EMV transaction functions are used, the device should evaluate the Application Usage Controls as "ATM".

To be consistent with today's Balance Inquiry processing, and with the EMV recommendations referenced in Section 5.9, the processing for ATM Balance Inquiry transactions is:

- An online request will be generated.
- To obtain information, the device will use the EMV-defined steps *Application Selection, Initiate Application Processing* and *Read Application Data*.
- For CVM List processing, the transaction is treated the same as an unattended cash transaction and the device will request the Online PIN.
- Card Authentication Method (ARQC generation) will be performed.
- The device will not continue with the rest of the EMV transaction sequence such as Terminal Risk Management and Terminal Action Analysis.
- The transaction should be completed with an Application Authentication Cryptogram (AAC), and not a Transaction Certificate (TC). Note: the AAC will not be passed to the host. The AAC will end the EMV transaction.
- When EMV transaction functions are used, the device should evaluate the Application Usage Controls as "ATM" and the CVM condition as "Unattended Cash".

For more information about the types of cryptograms that are used in EMV, refer to the EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 2.

5.9.2 Deposit/Cash Deposit

Deposit allows a cardholder to put funds into an account associated with the card. When EMV transaction functions are used, the device should evaluate the Application Usage Controls as "ATM" and the CVM condition as "Not Cash".

5.9.3 Funds Transfer

Funds Transfer allows a cardholder to move funds from one account associated with the card to another. When EMV transaction functions are used, the device should evaluate the Application Usage Controls as "ATM" and the CVM condition as "Unattended Cash".

5.9.4 PIN Change

The explicit PIN Change transaction may already be offered at U.S. ATMs for magnetic stripe cards, and can be offered for chip cards as well. A detailed discussion about PIN Change at the ATM will be included in a future version of this document.

5.9.5 PIN Unblock

The PIN Unblock issuer script is supported by most chip specifications. This provides a way to "unlock" the offline PIN in the chip. A detailed discussion about PIN Unblock is outside the scope of this document.

5.10 Network Considerations

Although most ISO/IEC 8583-based network specifications carry the bulk of EMV data in Data Element (DE) 55 (ICC Data), some do not. Some network specifications carry the EMV data in TLV format and some do not. It is therefore important to become familiar with the network specifications that are relevant to each specific financial institution.

Acquirers, networks, processors, and issuers that are prepared to handle EMV data will see a number of new data elements included in the authorization/financial messages.

The following items are generated during transaction processing or are supplied by the device and are used in cryptogram (ARQC) generation and validation:

- Amount, Authorized
- Amount, Other
- Terminal Country Code
- Terminal Capabilities
- Terminal Verification Results
- Transaction Currency Code
- Transaction Date
- Transaction Type
- Unpredictable Number

As previously noted, the original data elements that were used to create the ARQC must be passed through the network unmodified in order for the ARQC to be validated properly.

Although a great deal of information may be sent to the ATM by the card, the following items are involved in cryptogram generation and validation. They must be passed through the network unmodified.

- Application Interchange Profile
- Application PAN Sequence Number
- Application Transaction Counter
- Application Request Cryptogram (ARQC)
- Issuer Application Data

The following new data elements may be sent from the issuer in the authorization response to be delivered to the ATM:

- Issuer Script
- Issuer Authentication Data (which includes the Application Response Cryptogram/ARPC)

6 Recommendations and Suggested Best Practices

EMV has been implemented in many regions around the world, and many EMV Migration Forum members have been part of those implementations. As a result, some common themes have emerged. Although the EMV specification, global payment network specifications, and similar documents provide the framework for an EMV implementation, there are also "best practices" which are not covered in those documents. This section contains suggestions and recommendations based on experiences with EMV migrations around the world.

6.1 General Recommendations

Work closely with payment network representatives. Make sure the requirements of the individual payment networks are understood.

Work closely with vendors. Solicit their input and recommendations. Be aware of each vendor's plans and roadmaps for Windows XP to Windows 7 migration, software and kernel upgrades, recertifications, device drivers, and other updates.

If working with a processor, be aware of their EMV-readiness (for all relevant payment networks and brands). This includes both testing and certification of the processor's platform, and end-to-end testing to ensure compatibility between the processor and each make and model of ATM.

Clear business requirements are essential. Obtain sign-off from all the appropriate parties.

Allow extra time for all tasks that involve external vendors. Project delays are often related to external vendors, over which the ATM owner has little or no control. For example, a certification must be scheduled within a payment network's schedule; a hardware vendor may not be able to provide hardware or software when it is needed. Because so many external entities will be involved in an EMV migration project (e.g., hardware vendors, software vendors, payment networks), a delay on the part of one is likely to have a domino effect.

Those who wait to certify will undoubtedly find themselves in a queue with others who are trying to certify. This may cause significant delays in getting ATMs into production.

Although it may be tempting to consider migrating from Windows XP to Windows 7, or from Windows CE 5.0 to a newer version of Embedded Windows, while migrating to EMV, in reality, attempting both of these migrations at the same time is likely to be unmanageable and therefore is not recommended. An ATM owner may find opportunities to bundle minor changes with EMV, but may wish to consider avoid making additional major changes at the same time.

6.2 Technical Recommendations

6.2.1 Cardholder Selection

If the chip card only contains a single application in common with the ATM, the cardholder does not need to be presented with an application selection screen.

If the chip card only contains a single application in common with the ATM, but that application requires cardholder confirmation, the requirement can be met with an application selection screen (recommended).

If the card supports multiple applications that are also supported by the ATM, outside of implementations to support debit routing capabilities (i.e., “common debit application”), it is recommended that the ATM offer cardholder selection. A cardholder using an ATM is likely interested in accessing funds from a particular account associated with a particular application, which may not necessarily be the highest priority application on the card. For example, for a multi-product card, the credit application may be highest priority for use at the POS, but the cardholder may want to access funds from their debit account associated with the lower-priority debit application.

Unless the ATM deployer is providing business requirements to the kernel developer, it is likely that the ATM provider will have made the implementation decision as to whether Cardholder Selection will be offered. It is recommended that if the ATM provider has multiple offerings, some of which support Cardholder Selection, that the ATM deployer selects an offering with Cardholder Selection capability.

6.2.2 Global Payment Network Certifications

Many ATM processors have asked if it is feasible to perform EMV certification with one global payment network for an ATM, and move that ATM to production before certifying with other global payment networks to which the ATM processor belongs. There are several drawbacks to this approach.

For example, if an ATM is EMV M-TIP certified with MasterCard, a Visa chip card may be presented to the ATM. In this scenario, many, if not all, processors/financial institutions may treat this as a fallback transaction, because although the ATM is “EMV compliant”, the ATM does not have a Visa AID loaded on it. When the ATM reads the chip on the card, it will not find a match for the Visa AID(s) supported by the ATM, and the ATM will create a magnetic stripe transaction. Data elements in the online transaction request will indicate that a chip card was presented to a chip-capable ATM, but no matching AID was found. Some issuing processors and issuers may view this as a fallback transaction, with a correspondingly higher probability of declining the transaction. In addition, the acquirer may be subject to fines for excessive fallback processing, depending on applicable payment network rules.

Some ATM vendors offer something called a CAM field to assist in identifying AID mismatches, while other vendors may not offer such a field.

The EMV Migration Forum therefore recommends that when an ATM processor is certifying ATM processing for EMV, the scope of the effort should include certification with all EMV-ready payment networks (global and domestic) that are supported by the ATM. Where feasible, the ATM deployer may choose to place ATMs into production (or have EMV "turned on" for EMV-compliant ATMs already in production) only when all terminal certifications are complete for the majority of networks that the ATM supports. This will greatly reduce the possibility of AID mismatches, fallback, and unexpected fines.

6.2.3 Miscellaneous

Verify the hardware's power supply with the vendor. Stable power is critical (e.g., by using a UPS). EMVCo has specific requirements about voltage and other electrical characteristics of the terminal[17]. Under global payment network rules, the ATM must comply with EMV specifications when communicating with the chip.

Approved chip readers, and the expiration date of each, are listed under "Level 1 Contact Approved Interface Modules" on the EMVCo website (www.emvco.com). IFM approvals are given for a four-year period from the time of testing. At the end of four years, a four-year extension, or "renewal" may be requested (typically by the vendor). The EMV Migration Forum recommends that ATM owners/operators take note of the expiration date of any chip reader (IFM) they consider implementing, especially when purchasing used equipment. At the time of this writing, the global payment networks do not require that ATMs be removed from service when their chip reader's approval expires; however, the global payment networks do require that newly deployed ATMs contain IFMs and kernels with currently active approvals.

Approved EMV application kernels are listed under "Level 2 Contact Approved Application Kernels" on the EMVCo website. EMV kernels are given an approval with three-year expiration date, at which time a three-year renewal can be requested. The EMV Migration Forum recommends that ATM owners/operators take note of the expiration date of any application kernel they consider implementing.

Some ATMs maintain transaction logs to support research and trouble-shooting. The terminal provider should be consulted to determine the logging functionality (e.g., what type of logging is supported, how long data can be maintained). If the ATM is able to store transaction data, refer to Section 5.3 for a list of recommended data to log.

[17] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 1, Section 5

It is strongly recommended by the EMV Migration Forum, and may be required by some payment networks, to always support partial AID selection, as this is the only way to support multiple occurrences of applications. For more information about Application Selection and partial AID selection, refer to Section 7.2.

6.3 Ensuring a Positive Customer Experience

When implementing an EMV solution multiple hardware and software factors may impact the customer experience.

At the forefront, ATM providers should first consider if/how the ATM experience will change for:

- Customers using a magnetic stripe card versus those using a chip card
- On-us customers versus off-us customers; and whether ATM transactions will be acquired as EMV transactions for all cardholders (including on-us) or just off-us cardholders
- Customers using a motorized card reader versus a dip card reader

If there is a low volume of chip cardholders transacting on the ATM fleet, the ATM deployers may want to work with the application providers to limit customer experience impacts to those customers using a chip card while not impacting magnetic stripe card users. By adopting this strategy initially, the customer base will not be impacted until they are issued chip cards. Once the ATM deployer determines that the impact on chip cardholders is no longer acceptable, a different approach may be needed.

For ATM owners with motorized card readers in their ATM fleet, this approach will be transparent with regards to how the card is managed throughout the customer's session (since the card stays in the ATM device as long as necessary to communicate with the embedded chip). For ATM owners with dip card readers in their ATM fleet, one of two options will need to be implemented.

1. Since the chip card must be in contact with the chip reader, the dip card reader will need to 'clamp down' (i.e., hold on to the card) at initial card insertion. As such, any and all customers using chip cards will be impacted by a change in customer experience, not just those customers using cards on networks for which the ATM is currently certified.
2. An alternate approach for dip readers is the "double dip" method. This approach allows customers to initially dip and remove their card, enabling the application to read the magnetic stripe data to determine if the card being used is a chip card (via the Service Code). Customers using chip cards are then prompted to re-insert their card. At this point, the dip card reader will 'clamp down' (i.e., hold on to the card) for the duration of the transaction. Customers will then need to be notified when to remove their card. The "double dip" method allows the ATM owner to selectively manage the customer experience based on factors such as various network certifications, which may not occur all within the

same time frame. This approach also lowers the impact on customers who have chip cards, but those cards are not currently supported by the ATM fleet.

It is worth noting, however, that acquiring EMV transactions at the ATM may impact overall transaction times, to some extent, and may impact the user interface/screens presented to the cardholder regardless of the card reader type.

As stated previously in Section 4.2, EMV hardware selection can result in complexities with implementation and may impact the customer experience.

The following looks at each experience individually.

- Motorized card readers provide the most consistent customer experience and least impact when converting from magnetic stripe to EMV. The chip card in use will be held for the duration of the transaction; a new screen may be required while chip initialization takes place, and an additional screen will be required when cardholder selection is needed. The card can either be returned prior to the receipt printing or after.
- Dip card readers result in a different customer experience, particularly with regard to whether to prompt for card retrieval before cash is dispensed, or the reverse – dispense cash and then prompt for card retrieval. Each flow has its advantages and disadvantages to consider:

  "Card before Cash"

  Advantages: Customers must retrieve their card prior to obtaining requested cash and/or receipt, thus significantly reducing the likelihood a customer will leave their card behind. However, the EMV transaction must complete final communication to the chip before the chip card can be returned. This takes place much later than in the traditional transaction flow as the chip must remain in contact with the reader until this step is completed. Treating a motorized card reader as a "dip" reader (i.e., returning the card immediately upon card read) cannot be supported in an EMV transaction acquiring scenario.

  Disadvantages: In order for a customer to chain a set of transactions, they will be required to re-insert their card and as noted above, the card must remain in the card reader for the duration of the transaction versus the traditional approach which is to simply reconfirm the PIN.

  "Cash before Card"

  Advantages: Customers can perform multiple transactions in one session, since card is retained while cash and/or receipts are dispensed. Note: this also assumes that the additional "chained" transactions are supported by the AID selected. If not, the chip may

need additional interaction to determine the application to use and the transactions supported.

Disadvantages: Customers are more likely to inadvertently leave their card in the dip reader, thinking their transaction is complete.

6.3.1 Customer Communication

Prior to conversion from magnetic stripe to EMV, it is critical to communicate to customers and provide the appropriate level of education on EMV technology, highlighting key customer benefits. Consider all means of communication, such as direct mailings, emails, online web sites, mobile banking applications, and perhaps ATM attract loops and processing screens to highlight the pending migration and benefits. Customers tend to prefer a variety of media for the consumption of information. Strive for brevity, accuracy, and consistency among all communication vehicles.

- Emphasize the advantages of EMV technology, including:
  - Additional transaction security
  - Higher likelihood of transaction approval
  - Standard international technology for card transactions, now becoming a standard for U.S. card issuers
  - Future opportunities to offer multiple functions on the same card (e.g., loyalty programs, stored value)

6.3.2 Additional Considerations

6.3.2.1 New ATM Screens

As a result of the introduction of chip cards in the U.S., new ATM screens within the transaction flow will be necessary to guide the customer through the transaction. When implementing new screens and messages, ATM owners will need to update voice guidance (e.g., .wav files) as well.

6.3.2.2 Signage

Signage changes will further prepare customers for a change in their ATM experience. Signage may be as simple as an EMV chip decal on the ATM or more elaborate point-of-purchase displays informing customers that EMV transactions are accepted at this ATM. ATM providers may also want to provide information regarding chip card retention alerting customer that the card will be returned later in the transaction.

6.3.2.3 EMV-Specific Customer Service Phone Number

Additionally, providing a customer service phone number routed to EMV-educated specialists is advisable to answer any questions customers may have during the period of conversion. As with any

significant conversion, a broader marketing campaign may be desired for the smoothest conversion possible.

Customer-facing personnel, including branch personnel, should be trained so that they can assist customers who have questions about using their chip cards at the ATM.

7 ATM Transaction Processing with EMV

The EMV specification describes certain functions that are part of an EMV transaction, which is, a transaction initiated by a chip card at a payment-accepting terminal that supports EMV.[18] Some functions that are described in the EMV specification are applicable to an ATM transaction, and some are not. In this section, we will focus on the details of an ATM EMV transaction.

The following diagram shows the flow of a not-on-us transaction at a high level. The "Acquirer" icon actually represents any number of acquiring processors or gateways between the ATM and a payment network; similarly the "Issuer" actually represents any number of issuing processors or gateways supporting the authorization process.

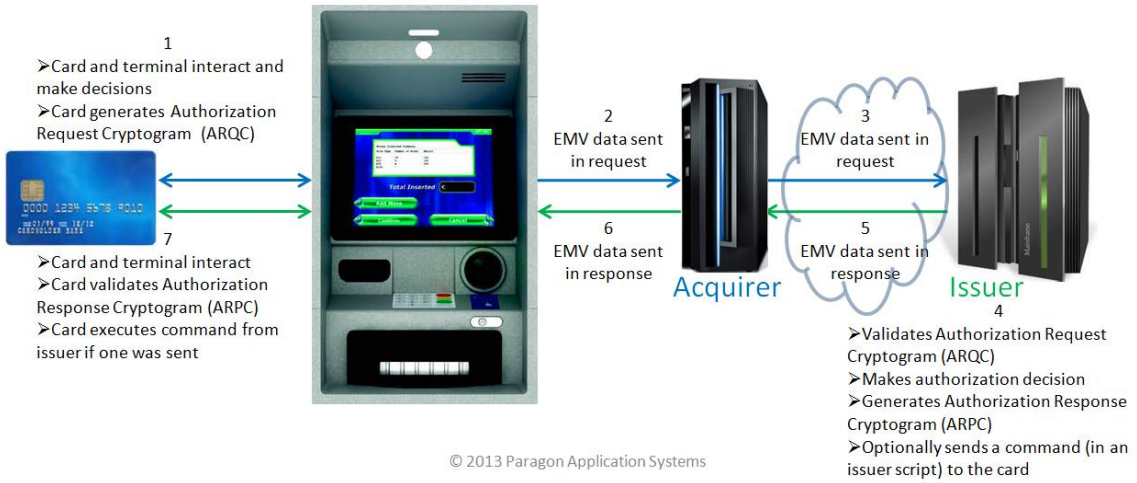

Diagram 7-1

The diagram below shows the steps involved in the interaction between the card and the terminal (Step 1 in the diagram above) during an ATM Cash Withdrawal[19]. The flows can be modified to address local requirements and particular situations. The functions are briefly discussed below, focusing on points particular to ATMs. The EMV flow is discussed in more detail in the EMV specifications.

As soon as the appropriate information is read during Step 1 in Diagram 7-1, and any time prior to Terminal Action Analysis, the device can process the steps 'Processing Restrictions' and 'Cardholder

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

[19] Only device functions are shown in the flow, not card functions such as *Card Action Analysis.*

Verification' in any order. Processes not defined by EMV, such as Transaction Selection, may be executed at any appropriate time.

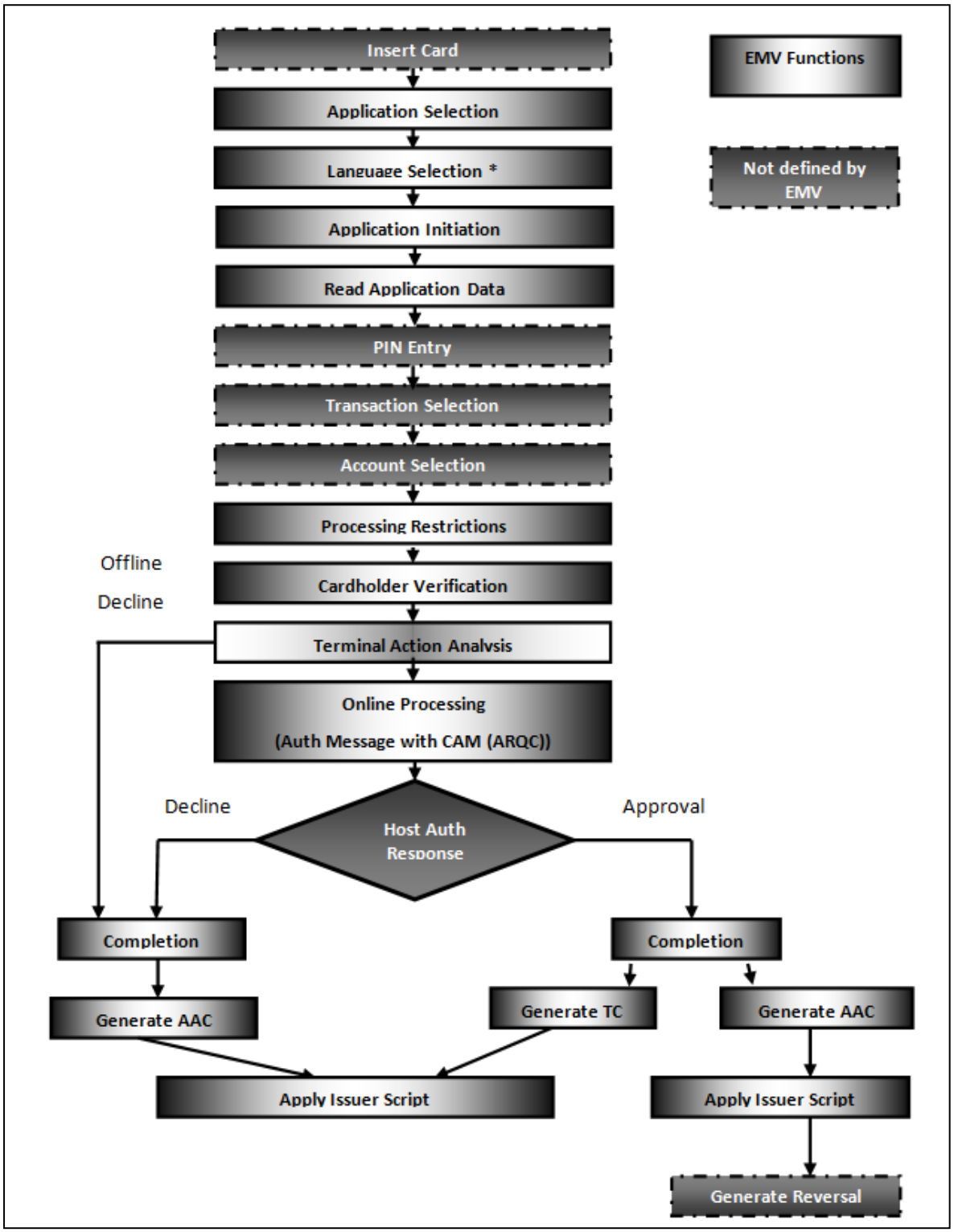

Diagram 7-2

7.1 Reading the Chip

The cardholder inserts their card to initiate the transaction. The ATM may examine the service code in the magnetic stripe, as discussed in Section 2.8.

Regardless of whether the ATM uses a motorized reader or a dip reader, once the ATM realizes that the card is a chip card, per the EMV specifications[20], it must attempt to communicate with the chip in the card. The chip has no power of its own; the power is provided by the ATM. The ATM will attempt to power up (activate) the chip and initiate an exchange of information.

Because there is a final exchange of information at the close of the transaction, the EMV chip card must remain in the reader until the information exchange is complete.

7.1.1 Fallback

The ATM is expected to always process the transaction using the chip if the chip is present and readable. “Technical fallback”, or simply “fallback”, means that the ATM is unable to complete processing the transaction using the chip, and so uses magnetic stripe processing to provide a service to the cardholder.

An acquirer may prefer this customer-friendly approach over rejecting the card at the ATM; and a payment network may even mandate that the acquirer create a fallback magnetic stripe transaction and pass it to the issuer rather than rejecting the card outright. The issuer would then be responsible for detecting fallback and taking the appropriate action.

As a reasonable balance between prioritizing the use of the chip and completing a transaction in a timely fashion, the ATM should attempt to retry accessing the chip a number of times (minimum of three) prior to falling back to magnetic stripe. If feasible, the ATM should attempt to restage the card in the chip reading station, or retract and re-land the chip reader (IFM) contacts in order to complete the transaction.

Fallback to magnetic stripe circumvents the improved security offered by EMV.

Note that some payment networks may not allow fallback, so that if the chip is inoperable, the transaction is terminated. Acquirers should refer to the requirements from the individual payment networks to decide how their ATMs will handle this situation.

[20] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 1, Section 6

In the initial stages of the U.S. EMV migration, higher levels of fallback are likely to be seen than in later stages of the migration, since some cards and terminals may not initially be configured properly. As the migration progresses, incidences of fallback should decrease.

7.2 Application Selection

Application Selection is the process mandated by the EMV specifications whereby the terminal and the chip card determine if they support any of the same ICC applications, and if they do, then agree on which application to use for the current transaction.[21] This is important for several reasons.

- Some applications are suited to ATM, some to POS, some to debit, and some to credit. If the card supports multiple applications, there may be different parameters and values for each application, and the ATM must use the right information for the transaction being initiated to ensure correct processing.
- Although the global payment network applications support the same basic core of EMV tags, using the same tag name, tag ID, length, and format, a specific payment network chip specification may also support proprietary EMV tags. For example, a MasterCard application may support a MasterCard-specific EMV tag.
- The format of some EMV tags can vary, depending on the chip specification (e.g., MasterCard M/Chip vs. Visa VSDC vs. American Express AEIPS vs. Discover D-PAS) and the associated application. For the most part, the ATM will simply be transmitting EMV data items to the acquirer for subsequent transmission to the issuer, but particular chip specifications may require the ATM to interpret the data from the chip.
- The terminal owner will be affiliated with some payment networks but may not be affiliated with others. If the card supports an American Express application, for example, but the terminal does not, then the ATM cannot use the data associated with the American Express application for this transaction. This is similar to a magnetic stripe transaction, in that if the acquirer is not authorized to accept American Express cards, it cannot proceed with a transaction if the magnetic stripe card only supports American Express.

As noted in Section 3.7, configuring the ATM to support EMV includes building a list of ICC applications (AIDs) that the ATM will support, and including that list in the device configuration. As part of the ATM's configuration for EMV, the Application Selection Indicator (ASI) value should be set. This field indicates whether the AID stored in the terminal must be the same length and value as the AID returned by the chip (meaning that only one match can be found for any payment network), or if the terminal can attempt to match by partial AID. It is strongly recommended by the EMV Migration Forum, and may be required by some payment networks, to always support partial AID

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

selection as this is the only way to support multiple occurrences of applications, as discussed in Section 2.3.

When the chip has been activated, the terminal will build what is called a candidate list, which is a list of all the AIDs the terminal supports that the chip also supports, and the priority of each. Per EMV specifications[22], there are two methods that a terminal can use to build the candidate list.

7.2.1 Payment System Environment (PSE)

Per EMVCo, this method is optional for the contact interface of a chip card; it is also optional for the terminal. Because PSE is more efficient than Explicit Selection (described below), an ATM that supports PSE will first send a command to the card to find out if the chip also supports PSE. If the chip does not support PSE, the chip will return a "file not found" response to the terminal. The terminal will then need to use the Explicit Selection method described below.

If the chip card supports PSE, a certain file will be present in the chip. The chip will return, in a single response, some information about all the applications the chip card supports; this includes the application name and its associated AID. Optionally, the chip may also send the Application Preferred Name, the Application Priority Indicator (API), Language Preference, and other information for each application it supports.

7.2.2 Explicit Selection (also known as List of AIDs)

If either the terminal or the card does not support PSE, or PSE is supported but the terminal is unable to find a matching application using PSE, the terminal must use the Explicit Selection method. Per EMV specifications, all EMV payment cards and payment-accepting terminals must support Explicit Selection[23].

The terminal will send a command to the card for each of the AIDs the terminal supports, and the card will respond, indicating whether the card supports the AID cited in the command from the terminal. For example, if the terminal supports ten AIDs, it has to send ten separate commands to the card and get ten responses back from the card. Each response indicates whether the chip supports the AID cited in the command; if the AID is supported by the chip, some information about the AID and its associated application is returned; for example, the dedicated file name and application label.

[22] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 1, Section 12.3

[23] Ibid.

If the card does not support a particular AID, it will return a "file not found" response to the terminal.

7.3 Final Selection

If the chip card and the terminal have no mutually-supported ICC applications, fallback to magnetic stripe may be allowed under relevant payment network rules.

As recommended in Section 6.2.1 Cardholder Selection, the terminal should support the ability to allow the cardholder to select an application or to confirm the application proposed by the terminal[24]. This is referred to as Cardholder Selection.

If there is only one mutually-supported application between the ATM and the chip card, or a domestic arrangement is in place to use only a particular application for domestic cards, Cardholder Selection is not necessary. In these cases, the ATM developer may wish to keep the user interface very similar to what is experienced today for magnetic stripe transactions. The flow may then look like Diagram 7-2, where PIN entry is requested immediately after card entry.

An ATM could perform logic such as:

- For a card with a single domestic chip application, that application is selected. Proceed with the existing user interface flow.
- If there is more than one application, the ATM proceeds with Cardholder Selection.

If only one application is supported by both the terminal and the chip card, and the Application Priority Indicator (API) is present in the chip for that application, the terminal uses information in the API to determine whether the terminal can automatically select that application, or whether the terminal must display information about the application to the cardholder and allow the cardholder to confirm the selection of this application.

7.3.1 With Cardholder Selection

Cardholder Selection may be implemented in one of two ways:

Menu

An ATM may use a menu to display all available applications to the cardholder and prompt the cardholder to select one. This is the recommended method for ATMs.

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

Single name

Alternatively, an ATM may display one application name at a time, which the cardholder can either accept or reject.

If the terminal and the chip card have more than one application in common, the terminal is expected to display the mutually supported applications and allow the cardholder to select the preferred application. The applications that have an API will be presented in priority sequence as indicated by the API, with the highest priority application offered first. Where the same priority is assigned to multiple applications, the terminal may present these applications in its own preferred order or in the order encountered on the card. For applications where the card's API is not present, the terminal may present these applications in its own preferred order or in the order encountered on the card.

7.3.2 Without Cardholder Selection

If the terminal does not have to offer a selection to the cardholder, then the terminal is expected to select the highest priority application that does not require the cardholder to confirm its selection. For example, if the terminal and the chip mutually support a single application, cardholder confirmation can be satisfied by including the Application Label and/or Application Preferred Name on the PIN entry screen.

While EMV specifications may allow the highest priority application among multiple applications to be used without allowing choice by the cardholder[25], some payment networks recommend (or may require) that if multiple applications are common between the ATM and the card, that the cardholder be given a choice (cardholder selection). A cardholder using an ATM is likely interested in accessing funds from a particular account associated with a particular application, and not necessarily the default of the highest priority application.

Although EMVCo recommends that each terminal should be prepared to display all of the applications that are mutually supported by the terminal and the card[26], issuers do configure the Application Priority Indicator (API) in the chip to indicate the "primary" application, which can be used to select the "preferred" application without cardholder input. However, a cardholder using a multi-application card anticipating a cash withdrawal from a checking account may be unpleasantly surprised by a cash advance against a credit line, if not given a choice.

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

[26] Ibid.

Once the application to be used is determined by the terminal or the cardholder, the terminal must notify the chip of this selection. A command is therefore sent from the terminal to the card to tell the chip which AID has been selected by the terminal. The chip then sends quite a lot of information about that application to the terminal, in the form of EMV tags. The terminal uses this information in some of the subsequent stages of the transaction.

Note that AIDs determine how data is retrieved from the card, while the RID component of the AID determines which TACs apply to this transaction. AIDs do not determine routing nor do they determine the processing performed by the acquiring host. Refer to Section 5.1 for more information about Application Identifiers and routing.

For more information on Application Selection, refer to the EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 1, Section 12.

7.4 Language Selection

The welcome screen at the ATM may display text in only one language, or in multiple languages.

The issuer may optionally specify from one to four languages that the cardholder prefers for each application on the card. As noted in Section 7.2, if an application on the chip houses a language preference, this information is passed from the chip to the terminal as part of the Application Selection process. If the terminal is configured to display information in multiple languages, it can interrogate the language selection options supported by the selected application, and display screens to the cardholder using the language which has the highest priority on the card that is, of course, also supported by the terminal. This will typically happen after the Final Selection process; up to that point, the ATM may display instructions in multiple languages until it has determined the application to use for the current transaction, and can therefore detect the cardholder's preferred language for a transaction that uses that application.

If no match is found and the terminal supports more than one language, the terminal may allow the cardholder to select the preferred language at the beginning of the transaction.

Local requirements may affect the display of languages.

7.5 Offline Data Authentication

Offline Data Authentication is not supported by ATMs today, so this step is not performed at an ATM. The terminal will update EMV Tag 95 (Terminal Verification Results, or TVR), to indicate that Offline Data Authentication was not performed.

ATM owners sometimes ask about supporting Offline Data Authentication in their ATMs. There are three types of Offline Data Authentication: Static Data Authentication (SDA), Dynamic Data Authentication (DDA), and Combined DDA/AC (DDA).

From a risk perspective, Online Card Authentication Method (CAM), in which an Authorization Request Cryptogram (ARQC) is dynamically generated to be checked by the issuer, is superior to **Static** Data Authentication (SDA), which only provides long-term protection against counterfeit cards. Unlike SDA, CAM uses dynamic components of transaction processing to provide better protection. When CAM is used, invoking SDA only increases processing time without providing additional safety.

Dynamic Data Authentication (DDA) also uses transaction data to protect against skimming. Just as CAM provides superior protection for online transactions, DDA provides superior protection for offline transactions.

Combined DDA/AC (CDA) is intended to protect offline transactions where there is significant opportunity for interception of chip-to-device communication.

Offline Data Authentication will have additional costs of implementation and ongoing key management, and will likely slow down transaction processing, with no additional risk benefits vis-à-vis CAM. Since the ATM's primary responsibility is cash disbursement, requiring online authorization requests, ATM owners do not need to implement Offline Data Authentication.

For more information on Offline Data Authentication, refer to the EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 3, Section 10.3.

7.6 Processing Restrictions

The purpose of the Processing Restrictions step is to determine the degree of compatibility between the application in the terminal and the application in the chip, and then note certain discrepancies for the issuer related to the following:

- Application version number
- Application expiration date
- Application effective date
- Application usage control

As part of the EMV tag for Application Usage Control, the card may be personalized to prevent use at the ATM. When the terminal detects this situation, an appropriate error message should be displayed, such as "This card does not permit ATM usage", and the transaction should terminate at this point.

Although it is possible to reject a transaction at the ATM if a discrepancy is detected between the application version number, expiration date, or effective date, most cards and terminals are configured (in the IAC and TAC, discussed in Section 7.11) to simply note any discrepancies that are found between the value of the item in the chip, and the value of the corresponding field in the terminal. The ATM then updates the TVR to reflect any discrepancies, and processing continues.

For more information on Processing Restrictions, refer to the EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 3, Section 10.4.

7.7 Cardholder Verification

Cardholder Verification is the process whereby the terminal, or the issuer, ensures that the person presenting the chip card is the person to whom the card was issued. EMV supports several forms of cardholder verification, for example, online PIN, offline PIN, signature, and "no cardholder verification required". Each application in the chip will have a Cardholder Verification Method (CVM) List that specifies which cardholder verification methods that application supports, and the order of preference as defined by the issuer.

Currently, no global payment network supports offline PIN use for ATM cash disbursements in the U.S. Since offline PIN is not currently used in an ATM, there is no need for the additional security requirements necessary to implement it at this time. For example, offline plaintext PIN support would require that the chip reader (IFM) meet many of the same high level of security requirements as are demanded for the Encrypting PIN Pad.[27]

Therefore, the only CVM that is used at the ATM at this time in the U.S. is online (DES-encrypted) PIN. If the CVM List for the selected application on the card does not include online PIN, the ATM transaction may not be able to proceed, depending on the relevant payment network rules.

If the selected application does support online PIN, this is often the point in the transaction where the cardholder is prompted to enter the PIN. In reality, it is up to the ATM owner as to exactly where in the transaction flow they want the cardholder to enter the PIN, as long as it is done before the ATM requests a cryptogram from the chip card.

Since an ATM always requests an online PIN for cash disbursement, some networks allow the ATM to request online PIN regardless of the CVM list on the card, and to include that PIN in the PIN block included with the authorization request. However, when the terminal performs a CVM that was not determined by the CVM list, in order to remain compliant with EMV specifications, the terminal will not set the TVR bits related to this CVM. In this case, if online PIN is not in the CVM List, the terminal updates the TVR to indicate that cardholder verification was not successful. Issuers will be aware of the appropriate payment network rules and process the transaction request accordingly.

Acquirers and cardholders are comfortable with online PIN processing today. The process of entering an online PIN is outside the boundaries of EMV processing, and the current process of PIN entry does not change with the introduction of EMV. If the PIN is entered into a secure Encrypting

[27] Devices that perform both POS and ATM functions may support additional CVMs, but this is outside the scope of this document.

PIN Pad (EPP), the PIN can remain in the EPP until needed for Online Processing (described in Section 7.14).

The encrypted PIN block is passed to the issuer (or on-behalf-of party) for verification, for both magnetic stripe transactions and EMV transactions.

For more information on cardholder verification, refer to the EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 3, Section 10.5.

7.8 Transaction Selection

This is often the point in the transaction where the cardholder is prompted to make any remaining selections, such as the type of transaction they wish to perform.

Not defined as part of EMV processing, Transaction Selection allows the cardholder to select the type of transaction that is to be performed. Choices typically include Cash Disbursement, Balance Inquiry, and Funds Transfer, as well as other functions provided by the acquirer. Cash Disbursement is the transaction type currently covered by the EMV specifications. Other transaction types, discussed later in this document, may take advantage of EMV functions.

7.9 Account Selection

Account Selection can be supported for chip transactions just as it is for magnetic stripe transactions.

Although not part of the EMV processing flow, Account Selection will generally follow Application Selection (and Transaction Selection). Account Selection allows the cardholder to select one of the multiple sources of funds associated with the primary account. For example, these accounts might include:

- Checking account
- Savings account
- Credit line account

Where the card and ATM have multiple applications in common, it is recommended that the Application Preferred Name (if the associated character set is supported by ATM) or the Application Label of the selected application be displayed on the Account Selection screen.

7.10 Terminal Risk Management

Terminal risk management is relevant for transactions that may be authorized offline, which would include some POS transactions, but not ATM transactions. The steps of terminal risk management are listed below.

- Floor limit checking
- Random transaction selection
- Velocity checking

None of these steps are necessary for an online ATM transaction. Since the floor limit for an ATM transaction is zero, all transactions go online for authorization. The ATM will simply indicate in the TVR in the online transaction request that terminal risk management was performed.

For more information on Terminal Risk Management, refer to the EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 3, Section 10.6.

7.11 Terminal Action Analysis

The chip card will typically have Issuer Action Codes (IAC) configured for each application on the chip. The IAC defines the action the issuer wants the chip to take under many different circumstances, as captured in the Terminal Verification Results (TVR – See section 2.10 Terminal Verification Results). The bits in the IACs mirror those in the TVR. Each IAC bit specifies an action to be taken if the corresponding bit in the TVR is set to 1 (“on” or “true”).

- Issuer Action Code – Denial
- Issuer Action Code – Online
- Issuer Action Code – Default

Similarly, a terminal will contain Terminal Action Codes (TAC). The purpose of the TAC is to define the action the terminal is to take under the same circumstances that are covered by the IAC. As with the IACs, the bits in the TAC mirror those in the TVR. Each TAC bit specifies an action to be taken if the corresponding bit in the TVR is set to 1 (“on” or “true”).

- Terminal Action Code – Denial
- Terminal Action Code – Online
- Terminal Action Code – Default

Each payment network (global and domestic) will define the set of TACs to be associated with their RID. Each set of Action Codes are associated with a phase of Terminal Action Analysis. In each phase, the terminal evaluates the relevant set of IACs and of TACs, and uses the most conservative choice to make a decision.

One of the actions determined by TAC/IAC processing is what type of cryptogram to request. Per the EMV specifications, there are three types of application cryptograms a chip can generate[28], but not all of them are appropriate for online transactions.

The only type of cryptogram that can be sent online to the issuer is the Authorization Request Cryptogram, or ARQC. Therefore, the terminal sends a command to the chip, requesting that the chip generate an ARQC and return it to the terminal for inclusion in the authorization request.

The IAC/TAC Denial codes specify the conditions under which the chip or the terminal will determine that the transaction cannot proceed; i.e., "are there any circumstances under which this transaction should not be processed?" The denial evaluation phase comes early in the transaction process. If a Terminal Verification Results (TVR) flag (bit) is set (as a result of processing that has taken place up to this point for this transaction), and the corresponding IAC – Denial bit is set or the corresponding TAC – Denial bit is set, the ATM will terminate the transaction at this point.

As an example, if the TVR flag is set for "Service Not Allowed" (because the card does not allow usage at an ATM), and the corresponding flag was set in the TAC-Denial (e.g. X'0010000000'), the ATM should terminate the transaction and display an appropriate error message, such as "This card does not permit ATM usage."

From a business perspective, an ATM will never decline a transaction offline; all transactions are sent to the host. Therefore, the logical setting in an ATM for each TAC – Decline Codes bit is zero.

The IAC/TAC Online codes specify the conditions under which a transaction will be sent online if a corresponding bit in the TVR has been set; i.e., "under what circumstances should this transaction be sent online?" As an online-only device, the only relevant setting to an ATM is "Transaction value exceeds the floor limit." Since the ATM floor limit is set to zero, the transaction will always go online and all other values in TAC–Online or IAC–Online are irrelevant. The terminal will now request a cryptogram (ARQC) from the chip card, prior to formatting the online authorization request. Per the EMV specifications (as an online-only device), ATMs are allowed to skip IAC/TAC Online processing if they always request an ARQC and always go online for authorization.[29]

The values in the TAC Default codes ("what is to be done if the transaction cannot be sent online?") will cause a transaction to decline if an online authorization cannot be performed. As an online-only device, the only relevant setting to an ATM is "Transaction value exceeds the floor limit." Since the ATM floor limit is set to zero, the TAC values should always cause the transaction to be declined if the ATM cannot go online. Per the EMV specifications, ATMs are allowed to skip IAC/TAC Default

[28] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 3, Section 6.5.5

[29] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 3, Section 10.7

processing if they always terminate the transaction when they cannot go online.[30] In any case, the transaction will be terminated. The logical setting in an ATM for each TAC – Default codes bit is zero.

ATM owners should check the various payment network specifications to determine the appropriate values for the TACs for a given application. As an example, for an ATM that supports Visa applications:

- The TAC – Denial values shall be X'0010000000'.
- The TAC – Online values shall be X'584004F800'.
- The TAC – Default values shall be X'584000A800'.

Note the deliberate use of the word "shall" above. In their operating regulations, the four global payment networks specify the TAC values that are to be used for their applications.

The TAC-Online and the TAC-Default do not need to be maintained in the ATM if the ATM skips TAC/IAC-Online and TAC/IAC-Default processing as described above.

[30] Ibid.

The following table includes the TACs for several payment networks, as known at the time of publication. Check with the payment network representative or hardware vendor to obtain the most current information.

Payment Network	RID	TAC-Denial	TAC-Online	TAC-Default
American Express	A000000025	0000000000	FFFFFFFFFF	FFFFFFFFFF
Diners Club/Discover	A000000152	Refer to Discover or terminal vendor for appropriate value	Refer to Discover or terminal vendor for appropriate value	Refer to Discover or terminal vendor for appropriate value
JCB	A000000065	0010000000	FC60ACF800	FC6024A800 or FC60242800
MasterCard (International)	A000000004	Refer to MasterCard or terminal vendor for appropriate value	Refer to MasterCard or terminal vendor for appropriate value	Refer to MasterCard or terminal vendor for appropriate value
Visa (International)	A000000003	X'0010000000'	X'DC4004F800' or X'584004F800'	X'DC4000A800' or X'584000A800'
Common U.S. Debit AID – Debit Network Alliance (DNA)	A000000620	TBD	TBD	TBD
Common U.S. Debit AID – Discover	A000000152	TBD	TBD	TBD
Common U.S. Debit AID – MasterCard Maestro	A000000004	TBD	TBD	TBD
Common U.S. Debit AID – Visa	A000000098	0000000000	FFFFFFFFFF	FFFFFFFFFF

Diagram 7-3

For more information on Terminal Action Analysis, refer to the EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 3, Section 10.7.

7.12 Card Action Analysis

When the card receives the command from the terminal with the request to provide an ARQC, the chip may perform its own risk management. Card risk management may include functions such as velocity checking, which are not relevant for an online ATM transaction. Details of the data and algorithms associated with card risk management are specific to the issuer and/or the entity whose ICC application is being used for the transaction. Refer to the individual chip specification (e.g., MasterCard M/Chip, Visa VSDC) for more information.

Based on the results of the card risk management functions, the card will determine the type of cryptogram to generate. Because ATM transactions go online, the card will only generate an ARQC in this scenario.

7.13 Cryptogram Generation

Each ICC application specifies exactly how cryptograms are to be generated and verified for that application; refer to the individual card specifications for the algorithms, EMV tags and other parameters that are used for each application. In general, the ARQC is generated using three components:

- The values of certain EMV tags, as indicated in the chip specification. EMV mandates a minimum number of EMV tags that must be used, but the individual chip specification is free to use additional tags. The tags are stored in the chip in the Card Risk Management Data Object List 1 (CDOL1), which is EMV Tag 8C. The tags that are used to generate the cryptogram include data from the card and data from the terminal. The majority of this data is dynamic; i.e., it changes for each transaction.
- A Card Master Key, also known as a key for authentication. Each chip specification may have a slightly different term for this key. This is a symmetric key which was derived from an issuer master key plus unique card data such as the PAN (or some portion of the PAN). This key is known only to the chip and the issuer (or an on-behalf-of/OBO party performing card authentication). The key is injected into the card when it is personalized for the individual cardholder. For sensitive actions such as ARQC generation, the chip will generate a unique session key that is based on the Card Master Key.
- A hashing algorithm (sometimes called a message authentication code, or MAC), which is used to reduce a large string of data to a more reasonable and manageable size.

The ARQC that is calculated by the chip will be a 16 character hexadecimal value.

The chip returns the cryptogram to the terminal, along with other information, including the type of cryptogram it is (e.g., ARQC).

The terminal formats its native mode message and sends it to the acquirer.

As part of the EMV configuration for the ATM, the acquirer will need to specify the EMV tags that the terminal is to send to the acquirer in each EMV transaction request. There will be a minimum set of tags as defined by EMV, which should be part of the default set of tags supported by the terminal vendor. The acquirer can send more EMV tags in the request, depending on the amount of tags that can be configured in the ATM, and the amount of information the acquirer wants to receive.

The way the EMV tags appear in the native mode message will vary, depending on the ATM software. For example, NCR and Diebold format the EMV tags in very different ways in their native mode messages.

For more information on ARQC generation, refer to the EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 2, Section 8, and the individual payment network chip specifications.

7.14 Online Processing

Once the native mode request message reaches the acquirer, the message will most likely be converted to another message format before sending it to an authorization system or a network. Many message formats pass EMV data in the original TLV format, but some message formats do not. In order to ensure correct processing, and to ensure that the cryptogram is validated properly, it is essential that the actual EMV tag value is not modified during this process. No values can be converted or translated. EMV tag values must reach the issuer (or OBO party) exactly as they left the terminal. The issuer (or OBO party) is the only entity with the key to decrypt the ARQC, so no other entity can translate or verify the ARQC.

In order to enable EMV processing, each entity in the transaction path must be able to pass EMV data. It is expected that each payment network will require that each connector certify with that network, to ensure that they can send and receive messages containing EMV data. In the U.S., a number of networks and processors have completed certifications with at least one payment network at the time of this writing.

Once the EMV transaction request reaches the authorization system, there are several steps that must be performed in addition to those already performed for magnetic stripe transactions. Because this document focuses on EMV implementation at the ATM, these steps are not described in detail here; however, the key steps are highlighted below.

7.14.1 PIN Verification

The PIN will be verified online. This is done the same way for all transactions initiated at an ATM, regardless of the technology (magnetic stripe transaction or chip).

7.14.2 ARQC Verification

By verifying the ARQC sent by the chip, the issuer ensures that the transaction was generated by a legitimate card.

The process of verifying the authenticity of the card is known as card authentication. The manner in which this is done is known as the Card Authentication Method (CAM). Because the chip generates the ARQC using dynamic data and a key known only to the chip and the issuer, this provides the highest protection against counterfeit and skimming.

Each payment network's card specification describes the data and algorithms that must be used to verify the ARQC for each application. Issuers will likely decline a transaction if the ARQC cannot be verified.

7.14.3 ARPC Generation

If the ARQC is verified successfully, the issuer may generate an Authorization Response Cryptogram (ARPC). Each payment network's card specification describes the data and algorithms that must be used to generate the ARPC for each application.

There are EMV-specific fields in the online transaction request that the issuer can use to determine whether the transaction was fallback, whether an issuer script was successfully executed in a previous transaction, and other actions taken by the card or the terminal. Many issuers will use the new EMV-specific data in the request as part of their authorization decision process.

7.15 Transaction Response and Completion

The issuer will send a response which will typically include the ARPC, and may optionally include an issuer script. The response will typically not include as much EMV data as the request. As with the request, it is important that all parties in the transaction path not modify any EMV tags as data is passed from one party to another.

The ATM will interrogate the response to see if it contains the EMV tag with the ARPC, or an EMV tag with an issuer script. If either is present, the ATM will pass the EMV tag(s) to the chip.

When the online authorization is completed, the ATM requests a final cryptogram based upon issuer response. An approval would result in a request for a Transaction Certificate (TC); a decline results in a request for an Application Authentication Cryptogram (AAC). Although ATMs are not required to retain the cryptogram (TC or AAC), requesting the final cryptogram is necessary to allow the chip to complete issuer validation.

If the issuer has approved the transaction but the card declines the transaction (the ATM requests a final cryptogram of a TC but the card returns an AAC), normally cash will not be dispensed. In this case, the ATM should generate a reversal to ensure the cardholder's account is not debited for the requested funds. Generally, this will occur only when there is issuer authentication failure.

7.15.1 Issuer Authentication

U.S. ATMs are on "Single Message" systems, where the authorization request is also the financial ("clearing") message. This single financial message will contain an ARQC, so there is no need to retain the TC.

The chip will attempt to verify the ARPC, if it is present. Successful validation of the ARPC proves that the response came from a legitimate issuer/authorizer. The issuer may personalize the card to decline the transaction if issuer authentication fails. This decision should always be made by the card per the issuer's personalization. Per EMV requirements, ATMs should never decline transactions simply because issuer authentication has failed, but rather follow the decision indicated by the card.

7.15.2 Issuer Script Processing (also known as Issuer-to-Card Script Processing)

If an issuer script is present, the chip will attempt to execute the command(s) in the script. Success or failure of this action is reported in an EMV tag that is part of the next online transaction performed by the card. The only exception is for the PIN Change transaction. A discussion of the PIN Change transaction is outside the scope of this document.

7.16 Reversals

Once a financial transaction request has been sent, if the transaction cannot be completed, a reversal should be sent to ensure the cardholder's balance is not improperly debited. Once EMV is implemented, new situations may arise where a reversal is needed. For example, as previously discussed, if a transaction was approved, but the chip is unable to successfully verify the ARPC, the chip may send an unsolicited status message to the terminal with a status code that indicates the problem (depending on chip personalization). If this prevents funds dispersal, the terminal should generate a reversal in this situation.

Reversals are not required, and should not be sent, for problems with issuer scripts[31], as reversals should be reserved for situations where all or part of the cash cannot be dispensed.

Refer to the individual terminal vendor EMV documentation for a list of possible status codes. For example, Diebold Agilis 91x uses their standard 912 unsolicited status messages.

[31] There is an exception for scripts containing PIN Change commands.

8 Conclusion

Migrating to EMV is a large and challenging project. In order to comply with mandates, and avoid the liability shift, ATM owners and operators should begin planning their migration process as soon as possible.

This document is intended as a general guide. Each ATM owner/operator will undoubtedly have unique needs. The EMV Migration Forum therefore encourages each ATM owner/operator to work closely with their vendors, processors, and payment network representatives to ensure a smooth transition to EMV.

9 Publication Acknowledgements

This white paper was developed by the ATM Working Committee of the EMV Migration Forum to provide an educational resource to stakeholders responsible for or interested in the implementation of EMV at the ATM in the United States.

Neither the publication of this document by the EMV Migration Forum, nor any of the recommendations or views expressed herein, constitutes, implies or should be construed to constitute or imply an endorsement of any of the member organizations of the Forum.

The EMV Migration Forum wishes to thank the ATM Working Committee members for their contributions.

The EMV Migration Forum thanks **Marc Cleven**, Visa, and **Deborah Spidle**, Paragon Application Systems, for leading the project, and the following ATM Working Committee members who wrote content for this document:

- Marc Cleven, Visa
- Craig Demetres, Chase
- Ron Schnittman, Bank of America
- Deborah Spidle, Paragon Application Systems

A number of contributors cannot be identified due to corporate policies, but are thanked for their work. The project team also recognizes the substantial commentaries provided by:

- Cathy Medich, Smart Card Alliance
- Bruce Wayne Renard, National ATM Council
- Coline Robert-Desestre, Galitt

Trademark Notice

10 References

10.1 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

10.2 Payment Networks

American Express

American Express technical specification web site:
http://www.americanexpress.com/merchantspecs

Debit Network Alliance

EMV Best Practices and Business Requirements for ATM Deployment:
http://www.debitnetworkalliance.com/bp.pdf

Discover

Contact your assigned Discover representative.

MasterCard

MasterCard Connect web site: https://www.mastercardconnect.com/

Visa

Visa Online web site for Visa clients: https://www.visaonline.com

Visa Technology Partner web site for vendors: https://technologypartner.visa.com/

Publicly available: Transaction Acceptance Device Guide: www.visa.com/tadg

10.3 EMV Migration Forum

Main page: www.emv-connection.com

Knowledge Center:

http://www.emv-connection.com/emv-migration-forum/knowledge-center/

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/

Future publications will include:

- PIN Change at the ATM
- An expanded discussion on Common AID support and routing

11 Glossary of Terms

AAC (Application Authentication Cryptogram) A cryptogram generated by the card at the end of offline and online declined contact transactions. It can be used to validate the risk management activities for a given transaction.

AC (Application Cryptogram) A cryptogram generated by the card in response to a GENERATE AC command, providing the card decision on the transaction. The AC is used to validate that the card has genuinely generated the response. The three types of cryptograms are Transaction Certificate (TC), Authorization Request Cryptogram (ARQC), and Application Authentication Cryptogram (AAC). The creation and validation of the cryptogram enables dynamic authentication.

ATM (Automated Teller Machine) An electronic telecommunications device that enables the clients of a financial institution to perform financial transactions without the need for a cashier, human clerk, or bank teller.

AEIPS (American Express Integrated Circuit Card Payment Specification) American Express' chip specification.

AID (Application Identifier) An alphanumeric representation of the application defined within ISO/IEC 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. Cards and 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).

ATM Provider An ATM owner or deployer.

APDU (Application Protocol Data Unit) Refers to the command message sent from the application layer within the terminal and the response messages returned by the card to the application layer within the terminal.

API (Application Priority Indicator) Indicates the priority of a given application or group of applications in a directory.

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

ARQC (Application Request Cryptogram) A cryptogram generated by the card at the end of the first round of card action analysis, which is included in the authorization request sent to the card issuer and which allows the issuer to verify the validity of the card and message.

ATR (Answer to Reset) After being reset by the terminal, the ICC answers with a string of bytes known as the ATR. These bytes convey information to the terminal that defines certain characteristics of the communication to be established between the ICC and the terminal. For more information, refer to EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 1, Section 8.

BCD (Binary Coded Decimal) A class of binary encodings of decimal numbers where each decimal digit is represented by a fixed number of bits, usually four or eight.

BIN (Bank Identification Number) 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.

CAM (Card Authentication Method) In the context of a payment transaction, the method used by the terminal and/or issuer host system to determine that the payment card being used is not counterfeit.

Cardholder Selection Process whereby the cardholder is presented with a list of the applications that the chip card and the terminal have in common, and is asked to select the application to be used for the transaction.

CDA (Combined DDA/Application (CDA) Cryptogram Generation) A card authentication technique used in online and offline chip transactions that combines dynamic data authentication (DDA) functionality with the application cryptogram used by the issuer to authenticate the card

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.

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. 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.

CVR (Card Verification Results) The chip card internal registers that store information concerning the chip card functions performed during a payment transaction.

D-PAS (D-Payment Application Specification) Discover's chip specification.

DDA (Dynamic Data Authentication) A card authentication technique used in offline chip transactions that requires the card to digitally sign unique data sent to it from the terminal. DDA protects against card skimming and counterfeiting.

DNA (Debit Network Alliance) A collaboration of U.S. debit networks whose goal is to provide interoperable adoption of chip technology for debit payments, while supporting security, innovation, and optimal technology choice.

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.

EPP (Encrypting PIN Pad) An apparatus that encrypts the clear PIN entered by the cardholder.

IAC (Issuer Action Codes) Codes placed on the card by the issuer during card personalization. These codes indicate the issuer's preferences for approving transactions offline, declining transactions offline, and sending transactions online to the issuer based on the risk management performed.

IAD (Issuer Application Data) An EMV tag that contains proprietary application data for transmission to the issuer in an online transaction.

ICC (Integrated Circuit Card) See chip card.

IEC (International Electrotechnical Commission) A non-profit, non-governmental international standards organization that prepares and publishes international standards for all electrical, electronic, and related technologies.

IFM (Interface Module) Also known as a chip reader.

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.

ISO (Independent Sales Organization) A third-party company that is contracted by a financial institution to procure new relationships.

ISO (International Organization for Standardization) An international standard-setting body composed of representatives from various national standards organizations.

LOA (Letter of Approval) Document issued to a vendor when the certifying agency approves the product being certified. The vendor may then advise their customers that the product has met the requirements of the certifying body.

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.

M/Chip. MasterCard's chip specification.

NFC (Near Field Communication) A standards-based wireless communication technology that allows data to be exchanged two ways between devices that are a few centimeters apart.

Not-On-Us A term used to mean "someone else's card at my ATM"; i.e., a card issued by an institution other than the institution (or an affiliate) that owns the ATM.

OBO (On Behalf Of) One organization may perform services on behalf of another.

On-Us A term used to mean "my card at my ATM"; i.e., a card issued by a financial institution (or its affiliates), used at an ATM owned by that financial institution (or its affiliates).

PCI (Payment Card Industry) Refers to the PCI Security Standards Council, an open global forum that is responsible for the development, management, education, and awareness of the various PCI security standards.

PAN (Primary Account Number) The payment card number.

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.

PKI (Public Key Infrastructure) The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.

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.

PSE (Payment System Environment) One method used to support Application Selection.

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.

SDA (Static Data Authentication) A card authentication technique used in offline chip transactions that uses signed static data elements. With SDA, the data used for authentication is static—the same data is used at the start of every transaction. This prevents modification of data, but does not prevent the data in an offline transaction from being replicated.

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.

TBD (To Be Determined) This acronym is used as a placeholder for information that is not yet available.

TC (Transaction Certificate) A cryptogram generated by the card at the end of all offline and online approved transactions.

TDES The Triple Data Encryption Algorithm (TDEA or Triple DEA), symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Also known as Triple DES.

TLV (Tag Length Value) Represents the format and order of information in an EMV data field (EMV tag).

TVR (Terminal Verification Results) The result of the risk management checks performed by the terminal during a transaction.

VSDC (Visa Smart Debit/Credit) Visa's chip specification.