Guidelines for Contactless ATM Transactions – A Guide for ATM Owners and Operators

Version 1.0

Publication Date: December 2018

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum, formerly the EMV Migration Forum, is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

About the ATM Working Committee

The U.S. Payments Forum ATM Working Committee explores the challenges of EMV migration for the U.S. ATM industry, works to identify possible solutions to challenges, and facilitates the sharing of best practices with the various industry constituents, with the goal result being more positive EMV migration experience for consumers.

EMV is a trademark owned by EMVCo LLC.

Copyright ©2018 U.S. Payments Forum and Secure Technology Alliance. All rights reserved. The U.S. Payments Forum has used best efforts to ensure, but cannot guarantee, that the information described in this document is accurate as of the publication date. The U.S. Payments Forum disclaims all warranties as to the accuracy, completeness or adequacy of information in this document. Comments or recommendations for edits or additions to this document should be submitted to: info@uspaymentsforum.org.

Table of Contents

1. Introduction

The objectives of this white paper, "Guidelines for Contactless ATM Transactions – A Guide for ATM Owners and Operators," are to provide guidelines for accepting contactless transactions at the ATM, and to develop best practices for contactless transaction interoperability for all ATM providers.

The U.S. Payments Forum ATM Working Committee understands that multiple definitions of "contactless" transaction are used in the market. This white paper focuses on contactless transactions completed with Near Field Communication (NFC)-enabled mobile wallets and contactless-enabled chip cards.

The white paper includes discussion of the following topics:

- ATM hardware requirements, including the multiple variations NFC readers.
- Software requirements, including contactless kernels and requirements for each contactless-enabled form factor (such as cards, mobile devices, wearable devices, rings, and key fobs).
- Network requirements for processing contactless transactions in the North American market.
- Interdependencies of the hardware and software.

This document is not intended to be a comprehensive textbook or step-by-step instruction manual, nor will it cover other transaction formats (such as QR codes). Also, Magnetic Stripe Data (MSD) contactless transactions, using any form factor, are out of scope.

The white paper does not discuss the security of contactless transactions.[1] Where relevant, the paper provides implementation recommendations and suggests industry contacts with whom to engage to help implement contactless transactions successfully.

This document provides guidance to ATM providers, acquirers, processors, and vendors who are preparing to implement contactless EMV transactions at their ATMs in the United States. The white paper also highlights how contactless EMV transactions differ from contact-based EMV transactions and covers contactless transactions using a plastic card, NFC-enabled mobile device, wearable device or other NFC-enabled form factor.

[1] For a detailed discussion of security, see the Secure Technology Alliance publication, "Contactless Payment Security Questions & Answers," available at https://www.securetechalliance.org/wp-content/uploads/Contactless-Payments-Security-QA-FINAL-Dec-2016.pdf.

2. Contactless Concepts

This section introduces basic contactless concepts, which are referenced in later sections of the document.

Contactless, for purposes of this white paper, is defined as the ability of two components (for example, a card and a card reader) to transmit data and communicate in close proximity using a radio frequency (RF) contactless interface.

Support for contactless functionality at the ATM provides the following benefits:

- Avoids traditional card skimming
- Allows a faster transaction
- Offers better convenience for consumers
- Delivers a platform for advanced ATM features; e.g., mobile/ATM integration
- Provides the same EMV level of security as contact for online authorizations, including the cryptogram

In summary, contactless transactions are fast, easy and secure.

2.1 Near Field Communication

Near Field Communication (NFC) is a set of standards defined by the NFC Forum[2] that enables proximity-based, low-power communications between consumer electronic devices such as mobile phones, tablets, personal computers or wearable devices. One device, the initiator, uses magnetic induction to create a radio-wave field that the target can detect and access, allowing small amounts of data to be transferred wirelessly over a short distance (within 4 cm).[3]

NFC relies on RF technology, which is widely used and is mature.

2.2 NFC Reader

A reader that supports NFC is required to perform NFC transactions at the ATM. Typical NFC readers consist of a main control board connected to an antenna board for receiving/transmitting NFC communications. The module is normally connected to the ATM processor via a USB port.

2.3 NFC and EMV Contactless Specifications

NFC and EMV are companion technologies. NFC applies to how devices communicate; EMV applies to how payments are made with contact and contactless chip cards or with an NFC-enabled mobile device emulating a contactless chip card. Contactless payment transactions made using NFC-enabled mobile devices use the same infrastructure as contact and contactless EMV chip card transactions.[4]

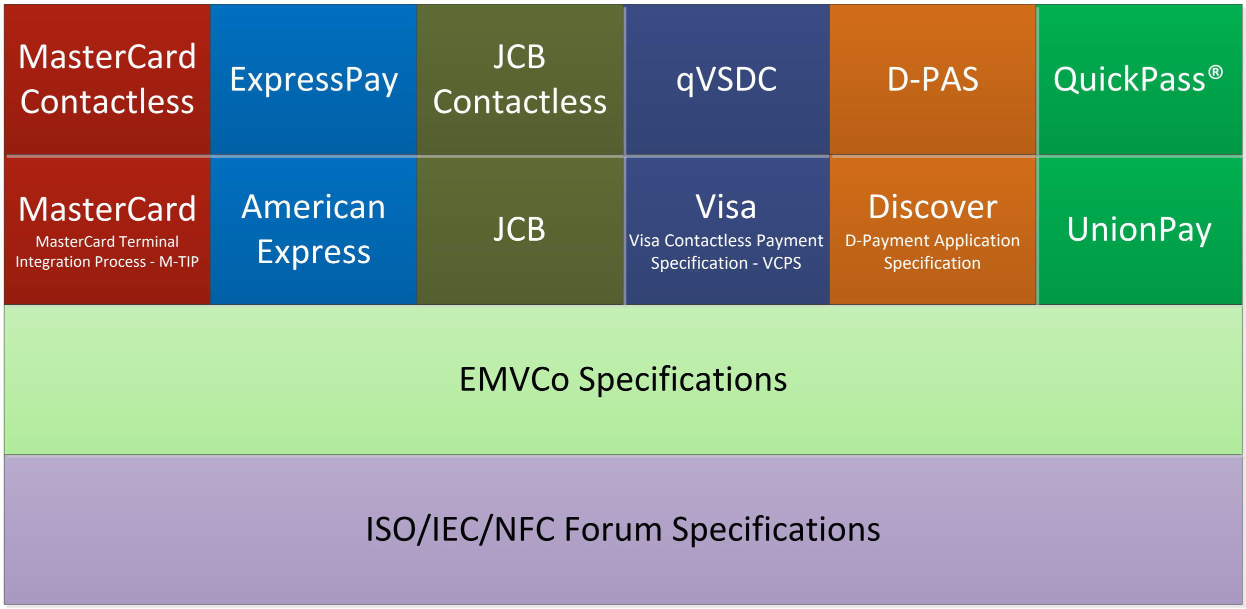
[2] NFC Forum website, http://www.nfc-forum.org/home.

[3] Referenced from the Secure Technology Alliance Glossary: Mobile and Contactless Payment Terms, January 16, 2017," and "Mobile and Contactless Payments Glossary," U.S. Payments Forum, September 2017, http://www.uspaymentsforum.org/mobile-and-contactless-payments-glossary/.

[4] "EMV and NFC: Complementary Technologies Enabling Secure Contactless Payments," Secure Technology Alliance, November 2015, https://www.securetechalliance.org/wp-content/uploads/EMV-and-NFC-WP-Final-Nov-2015.pdf

In summary, EMV is a payments technology and NFC is a communications technology that enables contactless EMV.

Figure 1 shows a graphical representation of the relationship between 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 contactless applications.



MasterCard Contactless

ExpressPay

JCB Contactless

qVSDC

D-PAS

QuickPass®

MasterCard
MasterCard Terminal Integration Process - M-TIP

American Express

JCB

Visa
Visa Contactless Payment Specification - VCPS

Discover
D-Payment Application Specification

UnionPay

EMVCo Specifications

ISO/IEC/NFC Forum Specifications

NOTE: EMV contactless specifications may be found on the EMVCo website.[5]

Figure 1. Relationship among EMVCo and Payment Network Specifications

2.4 Contactless EMV Kernels Concept

EMV kernels for contactless transactions are specific to payment network applications, which means different kernels must be implemented for each of the different networks that will be supported. For payment network certification, contactless differs from contact in that the Level 1 (L1) and Level 2 (L2) certifications are paired together when performing contactless transactions. NFC readers, similar to contact readers, require EMVCo Level 2 certification. Most NFC readers will already support an EMVCo Level 2-certified EMV kernel. ATM owners should be aware which payment networks are supported by the terminal.

When supporting contactless payments for the major payment networks, contactless hardware suppliers can accomplish L2 hardware certification using either of two different methods: payment-network-specific requirements or EMV contactless equivalents. Both are available for contactless hardware manufacturers, but ATM suppliers will typically only offer one option.

[5] https://www.emvco.com/emv-technologies/contactless/

As described in EMV Contactless "Book A: Architecture & General Requirements,"[6] the NFC reader may support the following kernels:

- C2 for Mastercard AIDs
- C3 for Visa AIDs
- C4 for American Express AIDs
- C5 for JCB AIDs
- C6 for Discover AIDs
- C7 for UnionPay AIDs

ATM implementers should confirm with the ATM manufacturer which kernels the NFC reader supports.

Support for Kernel C1 (for some cards with JCB AIDs and some cards with Visa AIDs) had been removed from EMV Contactless Book A, version 2.7. Visa and JCB AIDs are supported in Kernels C3 and C5, respectively.

2.5 Application Identifiers

The Application Identifier (AID) is used to uniquely identify each EMV application that a terminal supports. Every AID has an associated payment network and parameters relating to how the application needs to be processed.

AIDs are the same with contact and contactless payments. They differ in the following ways:

- For contact/integrated circuit card (ICC) applications, the AIDs are loaded in the Level 2 kernel running on the ATM's processor.
- For contactless applications, the AIDs and tags are likely to be loaded in the NFC reader itself:
  - As part of the EMVCo-defined kernels and already integrated as part of the NFC reader, or
  - Defined by the user and loaded in the NFC reader.

A list of the most common applications and their associated AIDs is available on the EFT lab website.[7]

2.6 EMV Contactless Tags

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

The EMV specifications define a minimum set of identifier tags that will be used or will be generated during EMV processing. For more information about EMV tags, refer to the U.S. Payments Forum white paper "Implementing EMV at the ATM."[8]

[6] EMV Contactless Specification, available on https://www.emvco.com/emv-technologies/contactless/

[7] A list of AID's with their description is available on the EFT lab website, https://www.eftlab.co.uk/index.php/site-map/knowledge-base/211-emv-aid-rid-pix.

[8] "Implementing EMV at the ATM," U.S. Payments Forum, available on http://www.emv-connection.com/implementing-emv-at-the-atm-requirements-and-recommendations-for-the-u-s-atm-community/.

Some payment networks have requirements for additional EMV tags that are used for contactless transactions.

A list of the most common EMV and NFC tags is also available at EFT lab website.[9]

For further information on EMV tags and their use, contact the payment networks directly.

[9] A list of EMV and NFC tags with their descriptions is available on https://www.eftlab.com.au/index.php/site-map/knowledge-base/145-emv-nfc-tags.

3. ATM Contactless Requirements

This section describes the ATM hardware, software, and configuration that are required to support contactless EMV transactions.

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 and/or contactless configuration for that equipment. Further, the ATM owner/operator should ensure that the ATM hardware/software providers understand the associated business requirements.

3.1 ATM Hardware

ATMs that do not currently support NFC readers will require an NFC reader to support contactless EMV transactions. The hardware vendor is responsible for obtaining Level 1 and Level 2 approval from EMVCo and/or the global payment networks. Refer to Section 4 and consult with the hardware provider on questions about NFC reader hardware, durability, and other operational requirements.

3.1.1 Support of Multiple Interfaces

For ATMs that can accept transactions over multiple interfaces, all permitted interfaces should be made available to the merchant/cardholder to perform a transaction. However, to prevent interference between the contact chip and contactless interface, the reader should always power down the contactless interface prior to the ATM device resetting the card to initiate a contact chip transaction. The contactless interface should remain powered down for the duration of the transaction that is conducted using the contact chip interface. Likewise, when the contactless interface is used, the ATM card slot should be disabled.

3.2 ATM Software

ATM deployers should check with their software provider(s) to determine whether their EMV-capable application software is compatible with the contactless configuration that they plan to deploy. Individually, each payment network requires a Level 1 and Level 2 Letter of Approval (LoA), and Level 3 certification. The ATM software itself does not require EMVCo testing or approval.

3.3 Contactless EMV Kernels at the ATM

Unlike contact chip, which has a single kernel that supports EMV transactions for all payment networks, contactless kernels are unique for each payment network, including the U.S. Common Debit AIDs for each of those networks where applicable. Each payment network will require certification of their individual contactless kernel to allow processing with their respective AIDs, including their U.S. Common Debit AID. For further information regarding the interaction of the kernel, the device and its components, please refer to the EMVCo website.[10]

Figure 2 shows the relationship among the ATM components that are involved in a contactless EMV transaction.

[10] https://www.emvco.com/emv-technologies/contactless/

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

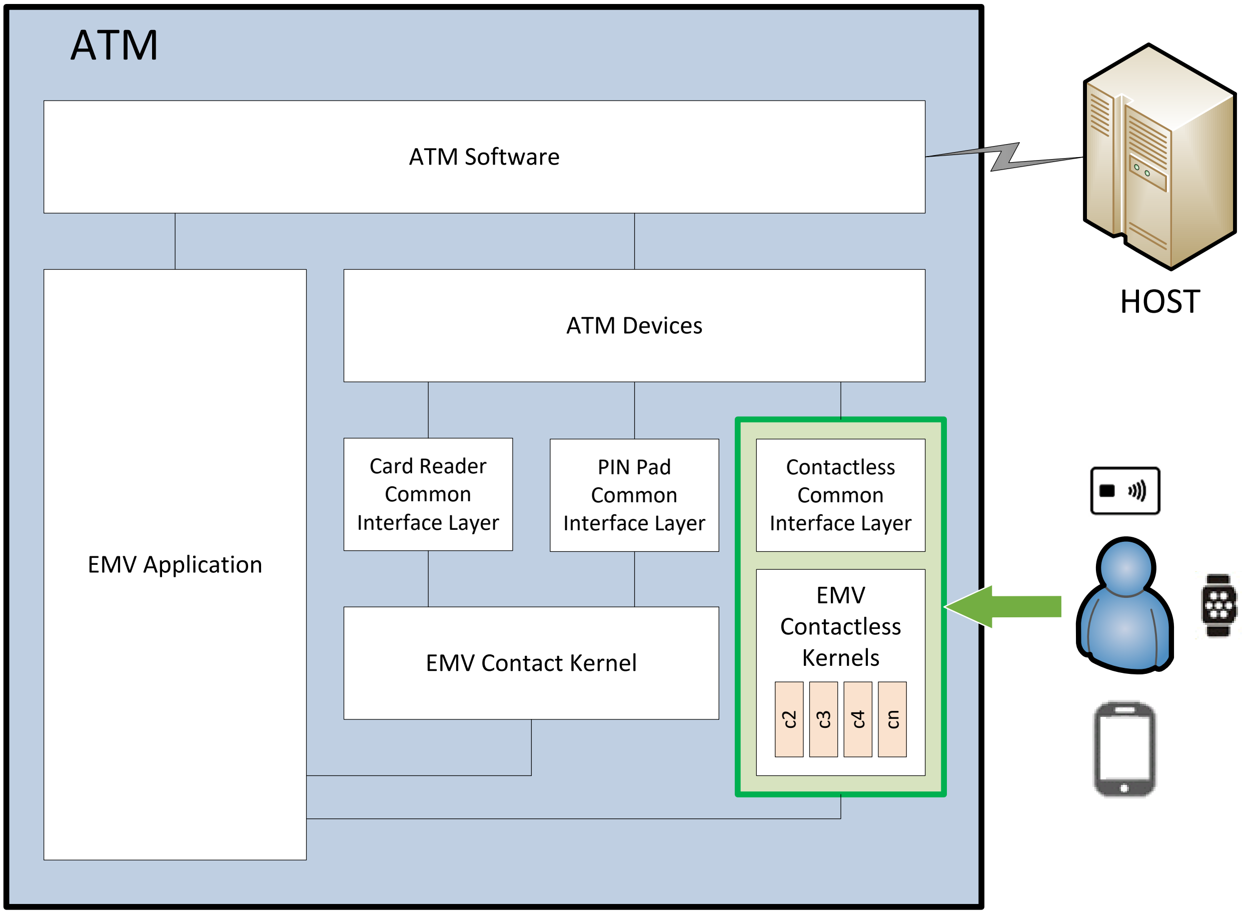

ATM
ATM Software
HOST
EMV Application
ATM Devices
Card Reader Common Interface Layer
PIN Pad Common Interface Layer
Contactless Common Interface Layer
EMV Contact Kernel
EMV Contactless Kernels
c2
c3
c4
cn

Figure 2. ATM Components Involved in a Contactless EMV Transaction

3.4 Configuration

Unique ATM characteristics need to be considered when performing contactless transactions. The following summarizes some of the important characteristics:

- Online authorization
  ATMs are online-only devices and always go online for Cash Disbursement and Balance Inquiry authorizations.
- No offline data authentication
  Because transactions are always sent online, ATMs do not perform offline data authentication.
- Online PIN
  The Cardholder Verification Method (CVM) used at an ATM is Online PIN; no other CVMs are currently supported for ATM transactions.

- Amount, Authorized

  The Amount, Authorized, also referred to as the Cryptogram Amount, is the amount sent from the ATM to the card for generation of the Authorization Request Cryptogram (ARQC). In most cases, during a contactless ATM transaction, the amount of the transaction to be authorized is not known at the time that the card sends the cryptogram data to the ATM, so the Cryptogram Amount is usually zero. Note: This means that the authorized amount and the Cryptogram Amount may not match.

- Transaction chaining

  ATMs often support transaction chaining, where a transaction is completed by offering another service. Re-tapping the card on the contactless reader's landing pad is:

  - Recommended by the payment networks for financial transactions, such as cash withdrawals and transfers, for security purposes.
  - Optional according to the payment networks for non-financial transactions for activities such as balance inquiries.

  However, for both types of transactions, re-entering the PIN is required by the payment networks.

- No data mixing

  For implementations where transaction data can be read from multiple interfaces, the transaction data should not be mixed in order to avoid data quality issues which may lead to a decline. For example, when a cardholder attempts to use the ATM for a contact chip transaction, the contactless reader may pick up the card data inadvertently. It is important to only use the data from only one interface.

- Certain transactions, particularly those that may involve scripting (e.g., for PIN changes), can be processed either by implementing a double-tap solution (not recommended) or by restricting these transactions to the contact interface only.

- Sales of goods and services and related transaction types, if performed at an ATM, fall under the payment network rules and procedures associated with point-of-sale (POS) transactions and are not considered ATM transactions. This will likely lead to the use of different processing parameters for purchase transactions conducted at the ATM.

4. Certification, Testing and Approvals Requirements

4.1 Testing and Approvals

NFC contactless reader and kernel approvals are normally obtained by the ATM vendor. Each ATM owner and/or ATM licensee should verify that the NFC contactless reader and kernels that they select have passed Level 1 and Level 2 testing. If not, certification will be required to support NFC contactless transactions.

4.1.1 Level 1: NFC Reader

NFC reader Level 1 testing includes Interface Module (IFM)/NFC reader functions (EMVCo Proximity Coupling Device (PCD) analog, digital and interoperability tests).

4.1.2 Level 2: Kernel

Kernel certification for each payment network supported at the ATM is required. Each network has a specific kernel, unlike contact chip where one kernel supports all EMV transactions.

As required by the payment networks, ATM operators will need to obtain all associated certification LoAs including but not limited to the ones shown in Table 1.

ATM operators should work with their contactless hardware supplier to ensure that the contactless hardware is still within the EMV L1 and kernel certification expiration dates.

Payment Network Specification	EMV Specification
EMV L1	EMV L1
Mastercard Contactless	C2 for Mastercard AIDs
VISA qVSDC[11]	C3 for Visa AIDs
American Express ExpressPay	C4 for American Express AIDs
JCB Contactless	C5 for JCB AIDs
Discover D-PAS[12]	C6 for Discover AIDs
UnionPay QuickPass®	C7 for UnionPay AIDs

Table 1. Contactless EMV Specifications

4.1.3 Level 3: Terminal Integration

Terminal integration approval, commonly referred to as Level 3 certification, depends on requirements set by each payment network.

[11] quick Visa Smart Debit Credit (qVSDC)

[12] D-Payment Application Specification (D-PAS)

Level 3 certification is intended to verify the implementation of security, conformance and interoperability within an integrated environment, including the terminal payment application, host protocol and specific data exchanged during an EMV/contactless transaction.

Terminal integration testing and certification can only be executed after all components and the host integration protocol are available.

Each network has a specific process for this certification, which normally requires the use of certified or qualified test tools, both to emulate cards or other NFC-enabled devices, as well as to simulate payment network and issuer messaging and responses in accordance with the defined test cases. (Check with the payment network to verify the tools that are available to support the integration.)

Besides Level 1, Level 2, and Level 3 approvals, other requirements may apply (e.g., Payment Card Industry PIN Transaction Security (PCI PTS) requirements, domestic debit payment network Integration).

Since adding NFC support is generally considered a major change to the payment application, payment networks may require a new Level 3 contact certification in addition to contactless certification.

5. Contactless ATM Transaction Processing

5.1 User Experience

Consumers will need some time to become familiar with the best way to tap their payment device at an ATM. During this initial period, depending on the transaction flow selected/defined, it is important that the terminal not abort the transaction too soon. To avoid negative user experience, the consumer should not have to abandon the transaction if the contactless transaction fails, but instead be given the opportunity to insert their contact chip card in the terminal to complete their transaction.

5.2 Card/Reader Interaction

EMVCo specifies that the interaction between the contactless payment device and the contactless reader must be completed within 500 milliseconds.

Additionally, EMVCo states that contactless cards, mobile devices and wearable devices must be readable at a distance up to 4 centimeters.

It is important to note that, prior to July 2016, some mobile devices received a Test Assessment Summary instead of a full LoA. In these cases, a waiver was issued by EMVCo in August 2014,[13] temporarily accepting failures at distances of 3 and 4 centimeters. As a result, some mobile devices tested prior to July 2016 may have issues with performing contactless transactions and have a negative impact on the user experience.[14]

5.3 Application Selection

Due to the short amount of time allowed for card/reader interaction, contactless ATMs will use the highest-priority application available on the card, except as noted below in section 5.3.1.

If multiple applications are supported in the candidate list, then payment networks specify the following process:

- The reader selects the application with the highest priority.
- Applications with an Application Priority Indicator (tag '87', bits 4-1) value of 0000b, or no Application Priority Indicator (tag '87') at all, are considered to be of (equal) lowest priority.
- In the case of multiple candidates with equal priority, the candidates are selected in the order listed in the Proximity Payment System Environment (PPSE).
- Cardholder application selection is not used in contactless transactions.

5.3.1 U.S. Common Debit AID

Currently in the United States, the U.S. Common Debit AID may supersede the global AIDs that may be on the card.

[13] Mobile Type Approval Bulletin No. 6, First Edition, August 2014, Mobile Level 1 Analogue Testing, Operating Volume, available on https://www.emvco.com/wp-content/uploads/documents/MTA_Bulletin_No_006-MobileLevel1AnalogueTesting-OperatingVolume_20140805045850407.pdf

[14] Mobile Type Approval Bulletin No. 12, First Edition June 2015, Mobile Level 1 Testing, Operating Volume , available on https://www.emvco.com/wp-content/uploads/documents/MTA_Bulletin_No_12-MobileLevel1Testing-OperatingVolume_20150702051424189.pdf

Under this process, when a card that contains the U.S. Common Debit AID and a global AID is presented at an ATM, the ATM may temporarily adjust the list of supported applications to only include the U.S. Common Debit AID, re-process the PPSE (which would result in the U.S. Common Debit AID being the only one shared by the card and terminal), and proceed.

Please note that per current payment networks requirements, this processing scenario is only permitted when a global AID is the highest priority on a debit card. If the global AID is highest priority on a credit card, even if the U.S. Common Debit AID is also on the card (for example, in the case of a card with multiple funding accounts), the global AID remains the highest priority.

For further information regarding U.S. Common Debit AID, please refer to "U.S. Debit EMV Technical Proposal."[15]

5.3.2 Multi-Funding Accounts

Some cards may be configured to support multiple funding accounts. For example, a card may be linked to both a credit account and a debit account. These cases can be detected when PPSE entries contain differing Issuer Identification Number (IIN, or Bank Identification Number [BIN] range) values. There may be a benefit to provide the cardholder with the option to select which account to use.

The payment networks recommend that issuers train cardholders with multi-funding accounts to not use the contactless interface and to insert the card (and use the contact interface) when they don't want to use the priority funding account in either POS or ATM environments.

For more information on the suggested implementation, see Section 6.4 of the "U.S. Debit EMV Technical Proposal."

If the implementation does not allow cardholder selection with multi-funding accounts, the default ATM behavior is to automatically select the account that has the highest priority AID. An exception to the default is if the BIN range associated with the highest priority AID is also associated with the U.S. Common Debit AID. In that case, the U.S. Common Debit AID may be selected.

5.4 CVM Processing

As discussed in Section 3.4, all ATM cash disbursement transactions must use online PIN as the CVM; however, ATMs must also be configured to not decline transactions because of CVM mismatches/failures. Additionally, PIN capture is not purely an EMV function and may be done outside of the kernel.

With contact EMV, payment networks recommend capturing the PIN prior to the terminal requesting the cryptogram from the card. With contactless EMV, since the interaction between the card and the reader must happen in a relatively short period of time, the PIN should be requested after the cryptogram is received from the card.

[15] "U.S. Debit EMV Technical Proposal," U.S. Payments Forum, available on http://www.uspaymentsforum.org/u-s-debit-emv-technical-proposal/

As a reminder, networks may differ in how the Terminal Verification Result (TVR) bits should be set for CVM processing with ATM transactions, and with contactless transactions in particular. Consult with each payment network supported to ensure correct CVM processing.

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

The EMVCo EMV tokenization specifications[16] specify PIN block support on transactions using payment tokens.[17] If an online PIN is used with a payment token, such as ISO 9564-1 PIN Block Format 0 or Format 3, the PIN Block includes the payment token in place of the PAN. The card issuer will receive the PIN Block with the primary account number (PAN) or payment token, as appropriate, for validation.

5.5 Default Amounts

Since the contactless card/reader interaction is completed quickly, a default amount for the Amount, Authorized tag will typically be used in cryptogram generation. This amount does not need to match the amount used in Field 4 of the authorization amount. Issuers will use the amount in Field 4 to decide whether to approve the financial transaction, but the Amount, Authorized data will be used to validate the cryptogram.

Payment networks recommend that the Amount, Authorized be set to a common value – e.g., zero.

If the contactless implementation allows the cardholder to enter the amount before the contactless card or mobile/wearable device is tapped, according to industry best practices, the amount entered should be used in the Amount-Authorized tag. Where possible, using the final amount is recommended, but not required.

5.6 Data Quality

To ensure correct processing and proper cryptogram validation, payment networks strongly recommend that the actual EMV tag values not be modified during the transaction process. (Check specific requirements with each of the payment networks.) No values are permitted to be converted or translated. EMV tag values must reach the issuer (or an on-behalf-of [OBO] party) exactly as they left the terminal, since the related validation is an end-to-end process. 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. Should any elements be inadvertently modified in the transaction path, correct authorization and processing may be compromised.

For contactless chip transactions (i.e., where POS Entry Mode indicates a contactless chip read), the value of all card-originated data used for the transaction is as read from the contactless chip interface.

With respect to Terminal Capability Code (TCC) or Terminal Entry Capability (TEC), it is recommended to contact the payment networks as the correct values may differ by payment network.

[16] "EMV® Payment Tokenisation Specification – Technical Framework," EMVCo, September 8, 2017, https://www.emvco.com/emv-technologies/payment-tokenisation/.

[17] Payment tokens are surrogate values that are substituted for PANS and used with NFC-enabled mobile phones with mobile wallets (e.g., Apple Pay, Google Pay, Samsung Pay) and other form factors.

5.7 Transaction Completion

Since the card and the card reader are not in contact at the end of a contactless transaction, the transaction completion procedures are typically quite different than contact EMV.

5.7.1 Issuer Script Processing

For contactless transactions, while script processing support is possible, it is not recommended by the payment networks for the following reasons.

- A double-tap would be required to support script processing, which can lead to a negative consumer experience and interoperability issues. Additionally, issuers have no way of knowing if an ATM supports the double-tap methodology, so they may not send scripts on contactless transactions.
- In the rare case that a script reaches an ATM, the device does not need to act on it. While specifications allow for an advice message to be sent from an ATM back to the acquirer acknowledging that a script was received and/or processed, this message is not required and rarely implemented.

Another option for ATM providers that wish to support scripting is to designate that transactions with scripts be completed using the contact interface. In this scenario, if the user selects a transaction that requires a script (e.g., a PIN change) after tapping the card, the ATM could direct the user to insert the card and use the contact chip interface.

5.7.2 Issuer Authentication (ARPC)

Similar to scripting, issuer authentication support (i.e., validating the Authorization Response Cryptogram [ARPC]) is not required in contactless processing, and is strongly discouraged by the payment networks. If an ARPC is received for a contactless transaction (which will be rare since issuers typically will not send it), the device may ignore it.

5.8 Tokens and Mobile Devices

Tokenization is the process of replacing the true card number (or true PAN) with a token that has the same format of a card account number, but is not an actual account number. Tokens are used in transactions initialized by mobile devices, wearables and other form factors.

From the perspective of the ATM, the actual processing of transactions initiated with a mobile device or wearable using a token is not significantly different from those initiated with a dual-interface or contactless chip card. The transaction should simply be packaged and sent to the acquirer.

The same is generally true for processors and acquirers unless these entities are tasked with connecting to the token service provider (TSP) for detokenization.

Processing tokenized transactions obviously requires that the transaction be detokenized at some point, so that the true PAN can be used in the authorization. The transaction will pass through the token service provider, which will detokenize the transaction and send it to the issuer or switch. The entity that is connected to the token service provider will have a BIN routing table that notes which BINs are for tokens and will route the transaction to the appropriate entity.

ATM deployers may want to identify the form factor if the customer is attempting a transaction that would be better suited to the contact interface. For example, if a mobile device is being used, directing the cardholder to insert a card may not be a viable option (for example, to complete a PIN change or conduct another transaction that requires scripting).

5.9 Receipts

There are no special considerations for contactless receipts that differ from the requirements for contact chip receipts. For more details about receipts, refer to the white paper "Implementing EMV at the ATM."[18]

5.10 Transaction Flows

Figure 3 and Figure 4 show the high-level flow for a "not-on-us" (or "interoperable") transaction. The "acquirer" icon actually represents any number of acquiring processors or gateways between the ATM and a payment network; similarly, the "issuer" icon represents any number of issuing processors or gateways supporting the authorization process.

The flows described can be modified to address local requirements and particular situations. The functions are detailed below, focusing on points particular to ATMs.

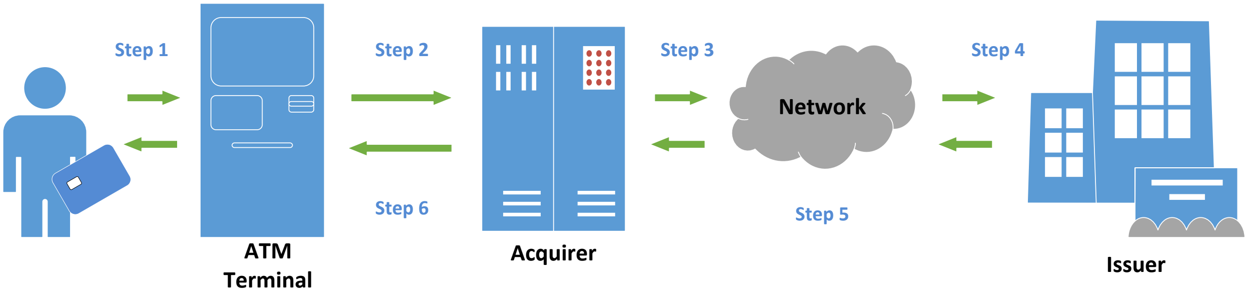


Figure 3. Contactless Card Form Factor (i.e., Non-Tokenized) Transaction Flow

Step 1:

- Customer taps a contactless card to initiate the transaction.
- A cryptogram is generated by the card and is passed to the ATM terminal.

Step 2:

- Transaction request is generated by the ATM and sent to the acquirer, including the PAN, the cryptogram, EMV tags, and other relevant transaction data.

Step 3:

- Transaction request is passed from the acquirer to the network.

Step 4:

- The transaction is sent to the issuer for authorization.

[18] "Implementing EMV at the ATM," U.S. Payments Forum, available at http://www.emv-connection.com/implementing-emv-at-the-atm-requirements-and-recommendations-for-the-u-s-atm-community/.

Step 5:

- The transaction authorization is sent back through the network to the terminal.

Step 6:

- The transaction is completed, the cardholder is notified of the result, and cash is dispensed.

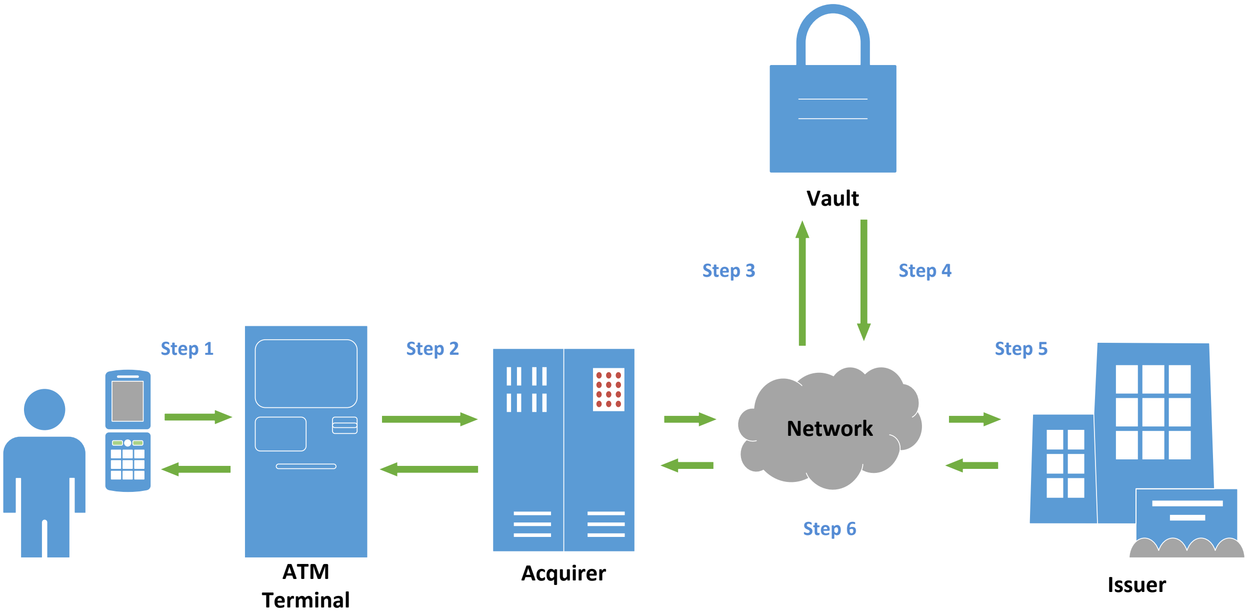


Figure 4. Mobile Device Form Factor (Tokenized) Transaction Flow

Step 1:

- Customer taps an NFC-enabled mobile device/wearable to initiate the transaction.
- A cryptogram is generated by the device and is passed to the ATM terminal. In place of the true PAN, a token is included in the transaction message.

Step 2:

- Transaction request is generated by the ATM and sent to the acquirer, including the token, the cryptogram, EMV tags, and other relevant transaction data.

Step 3:

- Transaction request is passed from the acquirer to the network.

Step 4:

- Transaction is sent to the token service provider vault for de-tokenization.

Step 5:

- The customer's PAN, token and transaction details are sent to the issuer for authorization.

Step 6:

- The transaction is completed, the cardholder is notified of the result, and cash is dispensed.

The ATM flow shown in Figure 5 illustrates a possible way to implement contactless transactions with a comparison to a typical contact transaction flow.

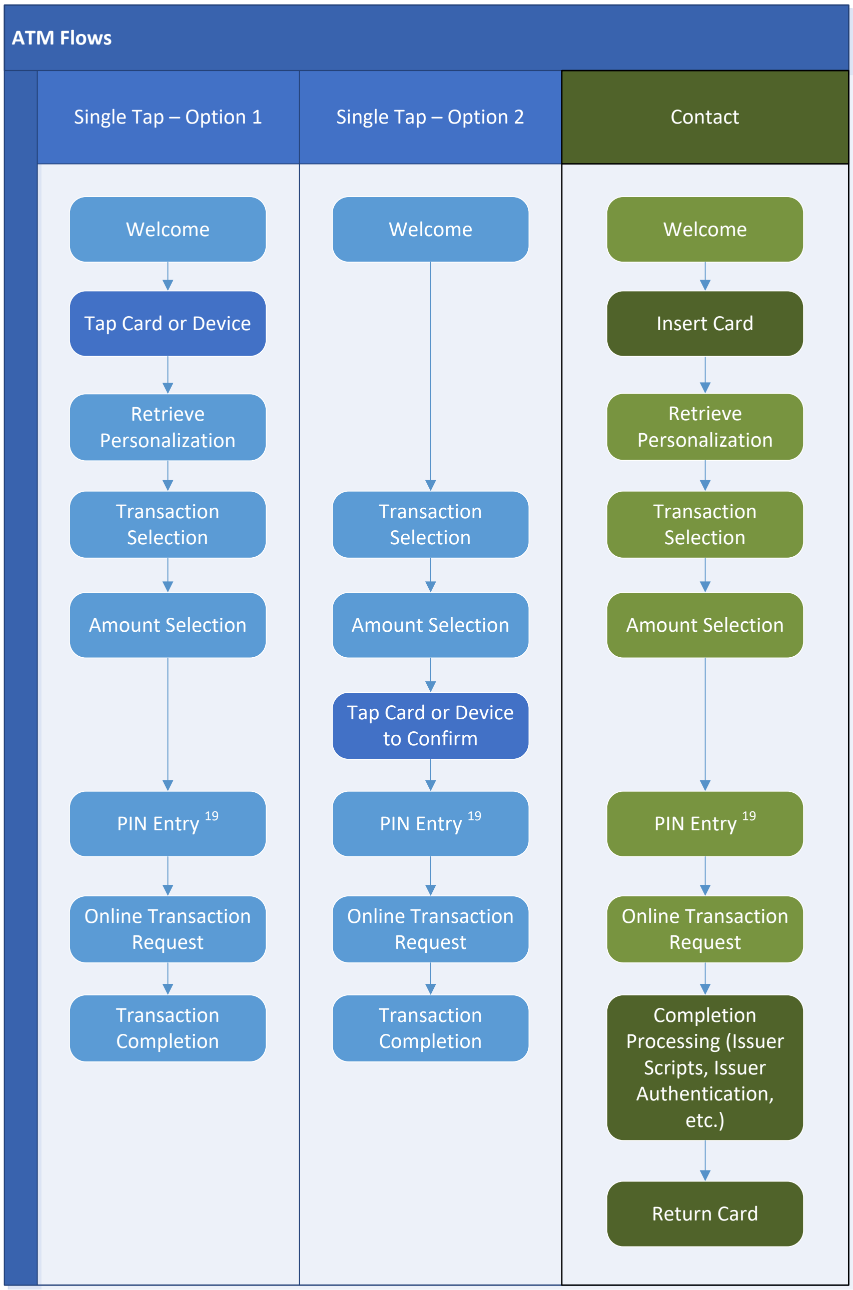


Figure 5. Example ATM Contactless Transaction Flow

The EMV transaction flow is discussed in more detail in the EMV Contactless Specifications, Book C, available on the EMVCo website.[20]

[19] Because it can take place outside of the EMV operations. PIN Entry may not take place in the sequence outlined in the flows above.

[20] EMV® Contactless Specifications, available at https://www.emvco.com/emv-technologies/contactless/.

6. Legal Notice

While great effort has been made to ensure that the information in this document is accurate and current, this information does not constitute legal advice and should not be relied on for any purpose, whether legal, statutory, regulatory, contractual or otherwise. All warranties of any kind are disclaimed, including all warranties relating to or arising in connection with the use of or reliance on the information set forth herein. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk.

Without limiting the foregoing, it is important to note that the information provided in this document is intended only to provide readers with an overview of challenges and issues that its contributors have encountered or believe are likely in connection with implementing EMV at the ATM. Each implementation is different, this document is not intended to be exhaustive, and applicable rules, processing, liability and/or results may impact or be impacted by specific facts or circumstances.

Additionally, each payment network determines its own rules, requirements, policies and procedures, all of which are subject to change.

ATM owners, ATM operators and others implementing EMV chip technology in the U.S. are therefore strongly encouraged to consult with all applicable stakeholders regarding their specific implementation plans and associated rules, requirements, policies and procedures for transaction processing, including but not limited to their respective payment networks, testing and certification entities, and state and local requirements.

7. Appendix I: References

7.1 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

7.2 Global Payment Networks

American Express

American Express technical specification web site:
https://network.americanexpress.com/globalnetwork/

Debit Network Alliance

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

Discover

Contact your PULSE Relationship Manager or visit https://www.pulsenetwork.com/

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/

Transaction Acceptance Device Guide: www.visa.com/tadg (publicly available)

7.3 U.S. Payments Forum

Main page: www.uspaymentsforum.org

EMV Connection: www.emv-connection.com

"EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community," U.S. Payments Forum Testing and Certification Working Committee, http://www.uspaymentsforum.org/emv-testing-and-certification-white-paper-current-global-payment-network-requirements-for-the-u-s-acquiring-community/

"EMV Troubleshooting Guide for ATM Owners and Operators," U.S. Payments Forum ATM Working Committee, http://www.uspaymentsforum.org/emv-troubleshooting-guide-for-atm-owners-and-operators/

"Glossary of Standardized Terminology," U.S. Payments Forum Communications and Education Working Committee, http://www.emv-connection.com/standardization-of-terminology/

"Implementing EMV at the ATM," U.S. Payments Forum ATM Working Committee, http://www.emv-connection.com/implementing-emv-at-the-atm-requirements-and-recommendations-for-the-u-s-atm-community/

"Implementing EMV at the ATM: PIN Change at the ATM," U.S. Payments Forum ATM Working Committee, http://www.emv-connection.com/implementing-emv-at-the-atm-pin-change-at-the-atm/

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

"Mobile and Contactless Payments Glossary," U.S. Payments Forum Mobile and Contactless Payments Working Committee, http://www.uspaymentsforum.org/mobile-and-contactless-payments-glossary/

"U.S. Debit EMV Technical Proposal, U.S. Payments Forum, http://www.uspaymentsforum.org/u-s-debit-emv-technical-proposal/

8. Appendix II: 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). A representation of the application defined within ISO/IEC 7816, technically defined as binary though typically implemented as alphanumeric. 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).

AID owner. An entity that licenses an AID, but is not a payment network. The Debit Network Alliance is an example of an AID owner.

ATM provider. An ATM owner, operator or deployer.

APDU (Application Protocol Data Unit). 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). EMV tag that 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). The first part of the card number/PAN that identifies the institution that issued a card. Also known as the IIN (Issuer Identification Number).

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 specifications have 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. EMVCo is responsible for 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 and to deploy POS and ATM terminals.

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.

Multi-AID card. A chip card that supports more than one AID. Support for multiple AIDs can be implemented in several ways, for example:

- **Multi-access card.** An application on the chip card is represented by more than one AID, and all of the AIDs pointing to that application are linked to the same funding account; e.g., a debit account.
- **Multi-product card.** A chip card that contains multiple AIDs that are not linked to the same funding account; e.g., one AID is linked to a debit account and a second AID is linked to a credit account. These accounts are typically represented by different PANs. Multi-product cards are sometimes referred to as "multi-funding" cards.

Multi-application card. A chip card that supports more than one ICC application.

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 "a different financial institution's credit/debit card used on another financial institution's ATM;" i.e., a card issued by an institution other than the institution (or ISO/affiliate) that owns/operates the ATM.

OBO (On Behalf Of). One financial institution organization who performs services on behalf of another.

On-Us. A term used to mean a financial institution's card used at that financial institution's ATM; i.e., a card issued by a financial institution (or its affiliates), used at an ATM owned/operated by or on behalf of 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 of 4 to 12 digits in length that is used to identify the cardholder upon entry 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 location where a retail transaction is completed, and at which a customer makes a payment to the merchant in exchange for goods or services.

PSE (Payment System Environment). One method used to support application selection.

RID (Registered Application Provider Identifier). First part of the AID. Used to identify a payment system 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) that are transported and identified by a tag which defines the meaning of the value, format, and length. The tag is simply a set of hexadecimal characters that identify the meaning of each piece of data transmitted between the ICC and the terminal.

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

TDES (Triple Data Encryption Standard). A 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). 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.