EMV® Migration Forum

WHITE PAPER

Implementing EMV® at the ATM:

PIN Change at the ATM

Version 1.0

Date: March 2015

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 PIN Change at the ATM

1.1 Executive Summary

Many U.S. issuers and acquirers do not offer PIN Change at the ATM today. Industry stakeholders often ask if an EMV migration project is a good time to implement this service. In order to make an informed decision, it is important for ATM owners and issuers to understand how PIN Change at the ATM functions in the magnetic stripe world today, and what should be considered when deciding if, where, when, and how to offer PIN Change at the ATM when implementing EMV.

This document provides guidance for ATM owners and issuers who are contemplating implementing PIN Change at the ATM as part of, or subsequent to, their U.S. EMV migration.

This document is being provided for informational purposes only and does not (nor should it be construed to) advocate adoption of a cross-bank or cross-network common PIN Change and/or PIN Unblock process, or any particular method for doing so. Note that adoption of any such process may depend on:

- Existing network PIN Change processes.
- Establishment of cross-network fee structures, which would require significant time, resources, and network-to-network negotiation.
- The ability of cardholders to determine which ATMs offer cross-bank, cross-network PIN change.

1.2 Additional Considerations

When considering PIN Change at the ATM, the following should be noted:

- Although this document includes business considerations related to PIN Change, at this time (March 2015) no acquirer has announced intentions to support PIN change for chip cards at ATMs in the U.S.
- PIN Change at the ATM is not mandated by any of the payment networks; however, some global network certification test plans may include PIN Change tests. An ATM owner who is not planning to offer PIN Change at the ATM may wish to obtain a waiver for any payment network certification tests related to this functionality.
- Cross-industry PIN Change processes (if any) that are developed and implemented in the U.S. may differ, and may involve considerations not addressed herein. Accordingly, the processes described in this document may differ from any related processes ultimately (if at all) that may be adopted.
- ATMs in the U.S. (and in other parts of the world) operate in an "online only" environment; that is, any request initiated at an ATM must be sent online to a host system for processing and approval. Even with the introduction of EMV, it is expected that ATMs in the U.S. will continue to operate in an "online only" environment for the foreseeable future.
- The chip card-related functionality described in this document is for contact chip cards, not contactless cards or the contactless interface on a dual-interface card. There is no definite direction for the implementation of contactless functionality at U.S. ATMs. In addition, some contactless EMV specifications do not support issuer scripts, which are an integral component of offline PIN management.
- U.S.-issued chip cards will continue to have a magnetic stripe for the foreseeable future. When the term "chip card" is used in this document, it means a card that contains a contact chip and also has a magnetic stripe.
- Although it is technically possible to assign a unique PIN to each ICC application on a chip card, issuers typically configure a chip card so that the same PIN is used by all applications on the card that require a PIN. This discussion assumes that a single PIN is used by all applications on a chip card that require a PIN, and that the online PIN and the offline PIN will always have the same value for a given card.

2 PIN Change in the Magnetic Stripe Environment

Some payment cards require the cardholder to enter a PIN when that card is used to perform a transaction. Today, very few (if any) U.S. payment terminals have the ability to verify the PIN entered by the cardholder. Therefore, when the cardholder enters their PIN at the payment terminal, the PIN is encrypted and sent as part of the online transaction request to a host system that does have the ability to verify the PIN. This verification is performed securely within a Hardware Security Module (HSM). Because the encrypted PIN is sent to a host system for verification, this process is known as online PIN verification, and the PIN that is encrypted and sent as part of the online transaction request is sometimes referred to as the online PIN.

Diagram 2-1: Online Magnetic Stripe ATM Transaction

The host system does not store the cardholder's PIN, either in the clear, or encrypted. Instead, the host system stores a value that is related to the cardholder's PIN; during online PIN verification, this value is used to verify that the cardholder entered the correct PIN at the terminal. There are several different ways to store the information that is used to verify the online PIN; these methods include using the PIN Offset, PIN Verification Value (PVV – Visa), or PIN Verification Number (PVN – Identikey). In this document, we will use the term PIN Offset to generically represent any of these PIN verification methods.

With a magnetic stripe card, the PIN Offset may be stored on the Track 2 of the card, or it may be stored on the issuer's host system. For obvious security reasons, the actual clear PIN is not stored anywhere on the card. The entire Track 2 from the magnetic stripe, which would include the PIN Offset if it is housed there, is sent to the host as part of an online transaction request. Therefore, if the PIN Offset is housed in Track 2 of the magnetic stripe, it does not have to be stored on the host system.

For various reasons, many issuers store the PIN Offset on the host, instead of in Track 2 on the card.

Having the PIN Offset in the magnetic stripe offers the issuer a quick (and usually "good enough") way to validate the PIN entered by the cardholder. However, this approach is falling out of favor; today, most issuers will use their HSM to take the encrypted PIN that comes in the transaction request, generate a PIN Offset, and compare that with the PIN Offset on file in a database. If they match, then the issuer is assured that the correct PIN was entered at the ATM. Issuers that continue to store the PIN Offset (or the PVV) on the card generally just reissue the card to implement a PIN change, or require the PIN change be done in the branch, which has a standalone magnetic stripe encoder which can re-write the entire track data on the card (including the new PIN Offset).

A magnetic stripe reader/writer that can update a high-coercivity magnetic stripe will generate strong magnetic currents. While some ATMs have in fact implemented a magnetic stripe encoder, it usually is reserved for updating Track 3 for the internal purposes of the bank.

Once a PIN change takes place, the previous PIN Offset value is rarely valid for the new PIN. If an ATM does not have a magnetic stripe encoder, the ATM cannot update the Track 2 of the magnetic stripe. Therefore, the issuer will store a value representing the PIN (such as a PIN Offset) in their database, and when a PIN Change is performed, update that value.

When the PIN Offset is stored on the host instead of the card, the PIN Offset is not captured if the magnetic stripe is skimmed from the card.

For these reasons, storing the PIN Offset on the card is falling out of favor. When a payment card is initially provided to the cardholder, a random PIN may also be generated for that card, and provided to the cardholder. The cardholder may want to change this random PIN to something that is more meaningful to them. Even if the cardholder has a "meaningful" PIN, after using their card for some time, they may want to change their PIN.

2.1 Where PIN Change Can Be Offered

There are several ways that an issuer can potentially allow a cardholder to change the PIN associated with their magnetic stripe payment card.

2.1.1 In the Branch

A cardholder may be able to go into a branch of their financial institution and change their PIN by using a hardware and software solution offered by the issuer. If the PIN Offset is stored on the card, the solution can calculate the new PIN Offset associated with the new PIN, and re-encode the magnetic stripe on the card. If the PIN Offset is stored on the host, the solution must pass information to the host so the new PIN Offset can be stored there.

2.1.2 Interactive Voice Response (IVR)

The issuer may allow the cardholder to call and change their PIN through an IVR. In this case, the PIN Offset would be stored on the host, since there would be no way to re-encode the magnetic stripe card at the time of the PIN Change.

2.1.3 At the Point-of-Sale (POS)

Although there may be no technical reason that PIN Change could not be offered at a point-of-sale terminal, for various business reasons this is generally not feasible. For example, an issuer may want the PIN Change function to be "on-us."

If the issuer does not acquire POS transactions, they will need to rely on one or more merchants, or very likely a merchant processor, to support PIN Change on their behalf. For reasons listed below, this may not be possible.

- Merchants want to get customers through checkout lines as quickly as possible, and therefore do not typically offer a service at the POS device that might take a few extra minutes.
- The cashier is not involved in this transaction, so the merchant may feel that they are paying the employee for time when the employee is not doing anything to actively assist the customer.
- The potential for shoulder-surfing and similar security risks is higher at the point of sale. At the ATM, customers who are waiting in line are likely to give the current ATM user sufficient space to perform their transaction in private, but this is normally not the case at the POS.
- If the PIN Offset is stored on the card, the POS terminal does not have the ability to calculate the new PIN Offset and re-encode the magnetic stripe. If the PIN Offset is stored on the host, the POS terminal would have to pass information about the new PIN to the host.

For reasons such as these, PIN Change is not usually offered in a POS environment.

2.1.4 At the ATM

The ATM is already the de facto unattended device used by cardholders to perform self-service functions today. These functions include relatively quick transactions such as a "fast cash" withdrawal, as well as functions that may require a bit more time. ATMs already offer both cash-dispensing and non-cash-dispensing functions. ATMs operate in an online environment, communicating with a host system for all transactions. It therefore follows that the ATM is a logical place to offer a self-service feature such as PIN Change.

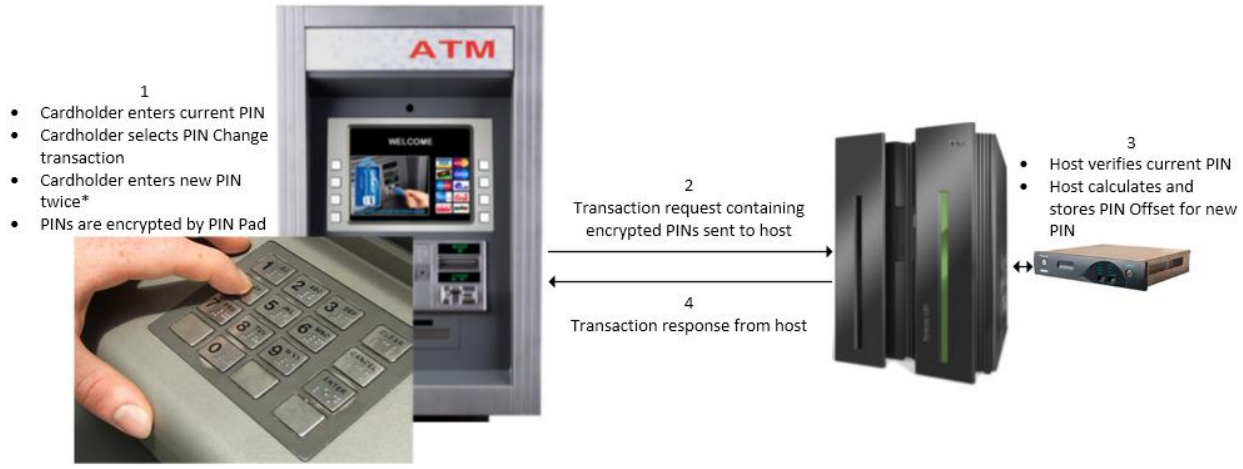
Whether the PIN is changed at the branch, through an IVR, or at the ATM, when the PIN is changed by the cardholder, the corresponding PIN Offset must also be updated. Neither the IVR nor the ATM can update the PIN Offset on the magnetic stripe on the card. Therefore if PIN Change is to be offered via IVR or ATM, the PIN Offset must be stored on the host system; it cannot be stored in the magnetic stripe on the card.

2.2 PIN Change Transaction Flow

PIN Change is a distinct transaction selection at the ATM; it is not combined with another transaction such as a cash withdrawal. The online PIN Change request message will therefore typically have a unique transaction/process/processing code, and the transaction amount will be zero.

Typically, the cardholder will select the PIN Change transaction at the ATM, enter their current PIN, and enter the new PIN twice, to make sure they enter the same new PIN both times. The current PIN and the new PIN are encrypted, and both encrypted PIN blocks are included in the transaction request that is sent to the host system.

The host will then typically verify the current PIN, and if the PIN is deemed valid, the host will generate the PIN Offset for the new PIN, and store that PIN Offset on the host system. The host will then generate a response to the ATM that confirms the outcome (approval or denial) of the PIN change transaction. If the response code indicates an approval, the ATM will display a message to the cardholder indicating that the PIN Change was successful.



* Depending on the implementation, the cardholder may be asked to enter the current PIN again after transaction selection, prior to entering the new PIN twice.

Diagram 2-2: Online Magnetic Stripe PIN Change Transaction

Customers who perform a PIN change at the ATM today are changing the online PIN that is associated with their magnetic stripe card.

2.3 PIN Change Scope

An issuer may support PIN Change at the ATM "on-us" only, that is, only at ATMs belonging to the issuer, and only for their cardholders.

PIN Change is sometimes available "in network," that is, at ATMs belonging to members of a certain network. In this situation, institutions belonging to that network have agreed that cardholders of any member institution may perform a PIN Change at any ATM belonging to any member of that network.

In rare cases, PIN Change may be offered at an ATM for any cardholder: on-us, or not-on-us (in network or out of network).

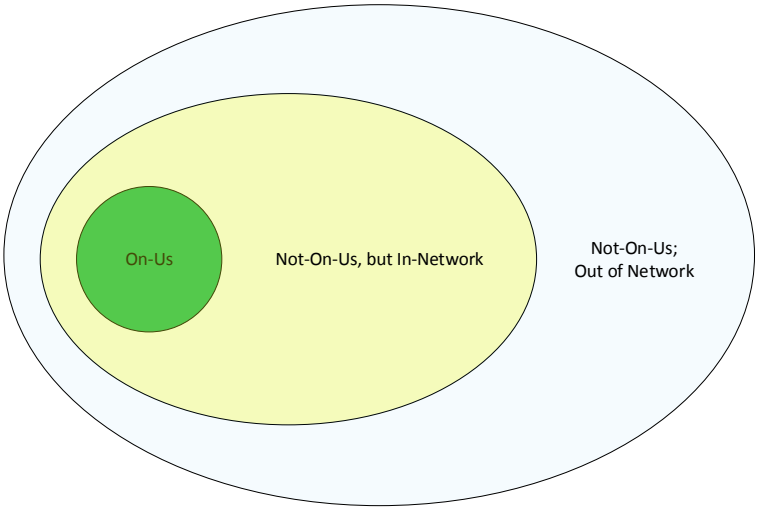


Diagram 2-3: Potential Scope for PIN Change

3 PIN Change in an Environment that Includes EMV

Even after the introduction of EMV, ATMs still operate in an "online only" environment. Transactions still go to a host system for authorization, and the encrypted PIN will still be sent to, and verified by, a host system. The diagram below shows the flow of an on-us EMV ATM transaction.

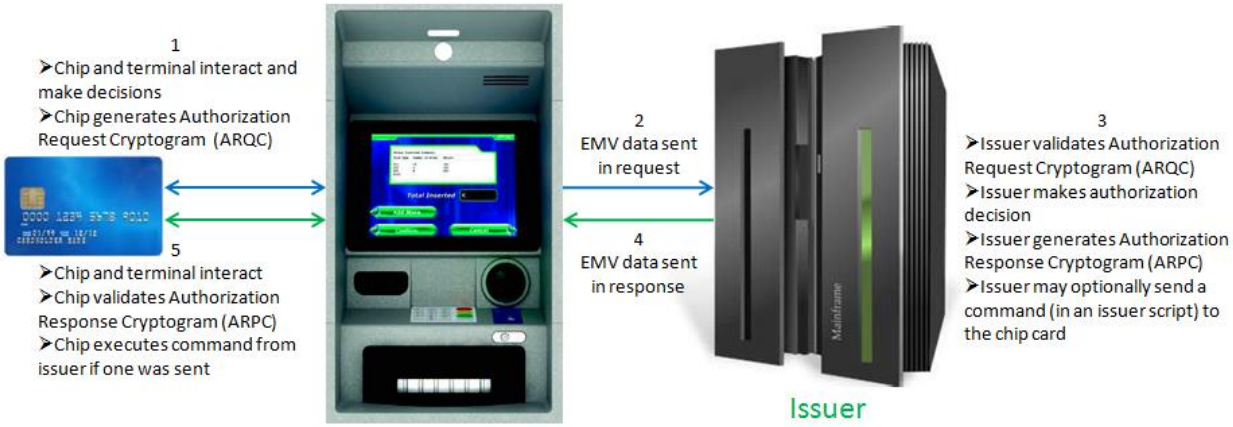


Diagram 3-1: EMV ATM Transaction

The greatest benefit of EMV is that it significantly reduces counterfeit card fraud. In an online transaction, this is accomplished by verifying the cryptograms (ARQC, ARPC) as seen in the EMV ATM financial transaction flow. By verifying the ARQC, the host is assured that the online transaction request was initiated by a legitimate chip card, since only the chip card and the host system have the key needed to generate and validate this cryptogram. By verifying the ARPC, the chip card is assured that the online transaction response came from the legitimate issuer.

But even if the host system can verify that the chip card itself is legitimate, that doesn't mean that the person using the chip card is the rightful cardholder.

3.1 Cardholder Verification Methods

The Cardholder Verification Method, or CVM, refers to the way in which the issuer (or terminal) verifies that the person using the card is the legitimate cardholder. The chart below shows that although several CVMs are possible at the POS, online PIN is the only CVM that is used today at the ATM.

Cardholder Verification Method (CVM)	Can be supported by Magnetic Stripe Card?	Can be supported by EMV Card? (Depending on the ICC Application)	Supported by ATMs?	Can be supported by POS Devices? (Depending on hardware and configuration)
Online PIN (Encrypted PIN sent online to host for verification)	Yes	Yes	**Yes**	Yes
Offline PIN (PIN verified between chip and chip-enabled terminal)	No	Yes	**No**	Yes
Signature	Yes	Yes	**No**	Yes
None (No CVM)	Yes	Yes	**No**	Yes

Diagram 3-2: EMV Cardholder Verification Methods

An ICC application in a chip may support more than one CVM. If the card is to be used at the ATM, the application should be configured to support online PIN as one of the available CVMs.

Some financial institutions may issue chip cards that support offline PIN verification. In this scenario, the PIN that is entered by the cardholder is verified between the POS terminal and the chip card. Because the encrypted PIN is not sent online to a host system and verified against the PIN Offset stored there, the PIN entered by the cardholder must be verified against a PIN that is stored in the chip.

Offline enciphered PIN verification requires the use of asymmetric keys and public key infrastructure (PKI). Offline PIN verification is not supported by ATMs today, and is optional at POS devices. Offline PIN verification is not mandated by EMVCo or by any of the payment networks. It is, however, widely used in some regions of the world, and may still be required by some payment-accepting terminals (e.g., at unattended kiosks for the transit system in France).

When a chip card contains multiple applications that require a PIN, or when the card supports both online and offline PIN verification, the same PIN is typically used by all applications on the chip card, since the cardholder would not know which PIN to use in any given situation.

If a chip card supports offline PIN verification, and the card can also be used in online transactions that require a PIN (such as at an ATM), then the PIN must be securely stored in the chip (for use in offline PIN verification), ***and*** the PIN Offset must be stored on the host system (for use in online PIN verification). When the card is used at a POS terminal that supports offline PIN verification, the PIN in the chip is used

to verify the PIN entered by the cardholder at the terminal, and in an online transaction requiring a PIN, the host verifies the PIN it receives in the online transaction request.

Although there is no technical reason why the online PIN and the offline PIN need to be the same for any given card, if these PIN values were different, the cardholder would not know which PIN to use in any given situation. Most likely the cardholder would not understand, nor be expected to understand, the difference between an online PIN and an offline PIN. This is particularly true at a POS terminal, where the cardholder would have no way of knowing whether the terminal supports offline PIN verification or not, so the cardholder would not know whether to enter the online PIN or the offline PIN. Therefore, the accepted best practice is to initially set the online PIN and the offline PIN to the same value for a card. Thus, regardless of where the PIN is changed, it is imperative for the PIN Offset that is stored on the host to be kept in sync with the PIN that is stored in the chip.

3.2 Where PIN Change Can Be Offered

Issuers that provide offline PIN support in their chip cards must provide a way for the cardholder to change the offline PIN. As with magnetic stripe cards, this can be done in the branch, via IVR (under certain conditions), or at the ATM.

3.2.1 In the Branch

As with magnetic stripe cards, a cardholder may be able to go into a branch of their financial institution and change their PIN by using a hardware and software solution offered by the issuer. For chip cards, the solution must have the ability to deliver the PIN Change issuer script to the chip card, to facilitate changing the offline PIN if the card supports offline PIN verification. The solution must also pass the new PIN (encrypted) to the host system so that the new PIN Offset can be calculated and stored there, and used for online PIN verification.

3.2.2 Interactive Voice Response (IVR)

The issuer may allow the cardholder to call and change the PIN associated with a chip card through an IVR. For chip cards, this is most often done only when the chip card is first issued, and a random PIN is assigned. The cardholder calls and selects their new PIN, and the host system is updated. The cardholder is then instructed to visit an EMV-enabled ATM and perform any transaction; the PIN Change issuer script will be delivered to the chip card with the transaction response, thereby updating the offline PIN in the chip. Subsequent PIN Changes for this card may not be allowed at the IVR.

3.2.3 At the Point-of-Sale

Although there may be no technical reason that PIN Change could not be offered at a POS terminal, for various business reasons (outlined earlier in this document) this is generally not feasible, for magnetic stripe cards or chip cards. PIN Change is therefore not usually offered in a POS environment, regardless of card or terminal technology.

3.2.4 At the ATM

The ATM is a logical place to offer a self-service feature such as PIN Change, for magnetic stripe cards and chip cards.

3.3 Offline PIN Management

The process of keeping the online PIN and the offline PIN synchronized is called offline PIN management.

As previously noted, PIN change is often offered at the ATM for customer convenience, offering a self-service way to change the PIN without having to come into the branch. Even though offline PIN verification cannot be used as a CVM when performing a transaction at an ATM, the ATM provides a convenient place to change both the online PIN and the offline PIN in a single transaction.

A major component of offline PIN management is the issuer script.

3.4 Issuer Scripts

Although there are several things about an EMV transaction that are different from a magnetic stripe transaction, one item that is particularly relevant to PIN Change at the ATM is the issuer script.

An issuer script is sent from the host as part of a transaction response when the issuer wants to update selected data in the chip. Through the use of an issuer script, the update can be made to the chip while the card is "in the field;" the cardholder does not have to bring their card into the branch, and the card does not have to be reissued. Only certain information can be modified in this way. Each of the payment network's chip specifications (e.g., M/Chip for MasterCard, VSDC for Visa) describes the EMV tags in the chip that can be updated through the use of an issuer script.

The issuer script, and the command(s) it contains, must conform to the Application Protocol Data Units (APDU) command-response format that is mandated by EMVCo, and recognized by the chip, since the script is sent unaltered from the host to the chip, and the chip only recognizes commands in APDU format.

In order to pass terminal certification, the ATM must prove that it is capable of passing an issuer script to the chip card. The ATM is just a conduit, passing the issuer script from the host to the chip to facilitate changing data that is stored in the chip. The ATM does not interrogate the contents of any issuer script.

When a chip card contains an offline PIN, the issuer must provide a way for a cardholder to change that PIN. A convenient way to do this is through the PIN Change function at the ATM. From the cardholder's perspective, PIN Change for the offline PIN is exactly the same as PIN Change for the online PIN. Typically, the cardholder selects the PIN Change transaction, enters their current PIN, and enters their new PIN twice. The PIN Change request, containing both encrypted PIN blocks, is then sent to the issuer. If the PIN change is approved, the issuer will calculate a new PIN Offset to match the new PIN, and update the PIN Offset on their host system. Additionally, if the PIN Change is for a chip card that

supports offline PIN verification, the issuer will return an issuer script that contains a PIN Change command, and the new PIN (encrypted). The ATM will then pass the issuer script to the chip, and the chip will execute the PIN Change command contained in the issuer script; this command updates the offline PIN that is stored in the card.

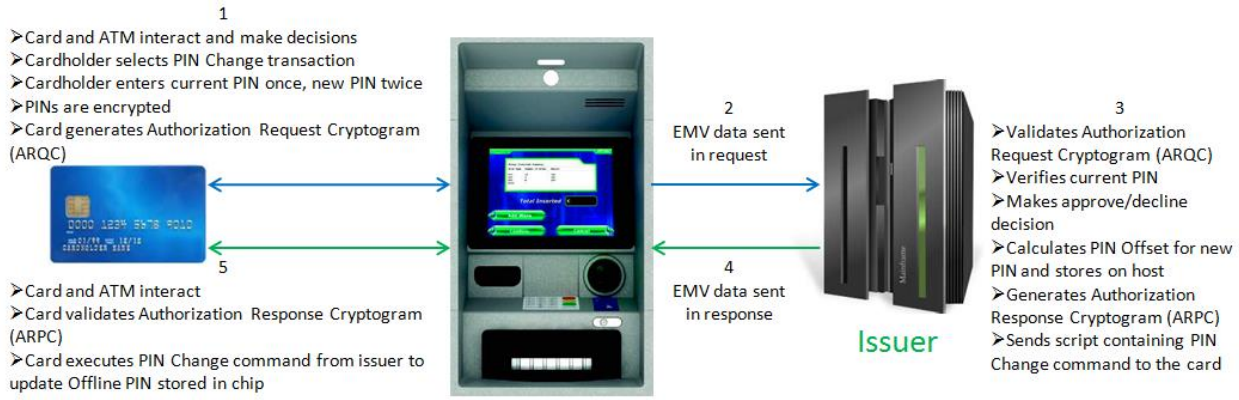


Diagram 3-3: Online EMV ATM PIN Change Transaction

If there is no PIN in the chip – i.e., if the chip card does not support offline PIN verification – then a PIN Change issuer script should not be sent to that card. PIN Change at a chip-enabled ATM by a magnetic stripe card, or by a chip card that does not support offline PIN, will update the online PIN. Magnetic stripe cards and ATMs that only support magnetic stripe cards cannot handle issuer scripts, so the offline PIN cannot be updated at the ATM unless a chip card containing an offline PIN is presented at a chip-enabled ATM that supports PIN change. Additional scenarios that must be considered when there is a combination of technology (magnetic stripe and chip) will be covered later in this document.

3.5 Comparison of PIN Change Transaction Flow for Magnetic Stripe and Chip

The following chart identifies the actions related to PIN Change that are the same (in green) regardless of card and terminal technology. Additional actions may be required, based on the combination of card and terminal technology, and whether the chip contains an offline PIN. Some actions taken by the ATM may be in a slightly different order than those shown here. This example assumes that the ATM is configured to read the magnetic stripe before attempting to read the chip, and that no errors or exception conditions are encountered (i.e., the cardholder enters a valid current PIN, and the chip is able to execute the issuer script from the host and update the PIN in the chip). The fallback scenario is addressed later in this document.

The expectation is that chip cards will continue to have a magnetic stripe on them for some time to come. Therefore, as stated in Section 1.2, the term "chip card" as used in the chart below indicates that the chip card also contains a magnetic stripe, but if the chip is successfully read, the transaction will proceed based on data in the chip.

Action	MS Card at MS-Only ATM	Chip Card at MS-Only ATM	MS Card at Chip ATM	Chip Card at Chip ATM – Chip Does Not Contain Offline PIN	Chip Card at Chip ATM – Chip Contains Offline PIN
Cardholder inserts card	Yes	Yes	Yes	Yes	Yes
ATM checks service code in magnetic stripe to determine card technology	n/a	n/a	Yes	Yes	Yes
ATM successfully reads chip	n/a	n/a	n/a	Yes	Yes
Cardholder selects explicit PIN Change transaction	Yes	Yes	Yes	Yes	Yes
Cardholder enters current PIN once	Yes	Yes	Yes	Yes	Yes
Cardholder enters new PIN twice	Yes	Yes	Yes	Yes	Yes
PINs are encrypted and sent to host	Yes	Yes	Yes	Yes	Yes
Host verifies current PIN	Yes	Yes	Yes	Yes	Yes
Host calculates new PIN Offset and stores on host	Yes	Yes	Yes	Yes	Yes
Host generates PIN Change issuer script if offline PIN is supported	n/a	n/a	n/a	n/a	Yes
Host sends response to ATM	Yes	Yes	Yes	Yes	Yes
ATM forwards issuer script (if present) to chip	n/a	n/a	n/a	n/a	Yes
If chip receives an issuer script with PIN Change command, chip updates PIN in chip	n/a	n/a	n/a	n/a	Yes
Appropriate "success" message displayed to cardholder	Yes	Yes	Yes	Yes	Yes
Cardholder removes card when finished	Yes	Yes	Yes	Yes	Yes

MS = Magnetic Stripe
Yes = this step occurs in this scenario
n/a = this step is not applicable to this scenario

Diagram 3-4: PIN Change for Magnetic Stripe vs. Chip

As indicated in the chart above, magnetic stripe cards, and magnetic stripe-only ATMs, cannot handle the new EMV data; this includes issuer scripts from a host.

An ATM owner that supports PIN Change today for a magnetic stripe card at a magnetic stripe-only ATM will continue to use their current process going forward, conducting business as usual.

Similarly, if a chip card is presented at an ATM that is not yet chip-capable, the ATM will create a magnetic stripe transaction, since it cannot read the chip on the card. If the cardholder selects the PIN Change function, the PIN that will be changed is the online PIN, and the PIN Change process is the same as for a magnetic stripe card at a magnetic stripe-only ATM.

If a magnetic stripe card is presented at an ATM that is EMV-enabled, the ATM will create a magnetic stripe transaction, since there is no chip on the card. If the cardholder selects the PIN Change function, the PIN that will be changed is the online PIN, and the PIN Change process is the same as for a magnetic stripe card at a magnetic stripe-only ATM.

If a chip card is presented at an EMV-enabled ATM, and the chip is successfully read, and the cardholder selects the PIN Change transaction, the ATM will format an EMV transaction, which will be sent to the host. The host must determine whether the chip card supports offline PIN verification (and therefore contains the offline PIN in the chip) or not. If the chip supports offline PIN verification, the host must format a PIN Change issuer script and include it with the response that is sent back to the ATM. If the chip does not support offline PIN verification (and therefore there is no PIN in the chip), the host will not send an issuer script with the response. In either case, the PIN Offset that is stored on the host system must be updated so that it remains synchronized with the PIN known to the cardholder and the PIN stored in the chip (if present).

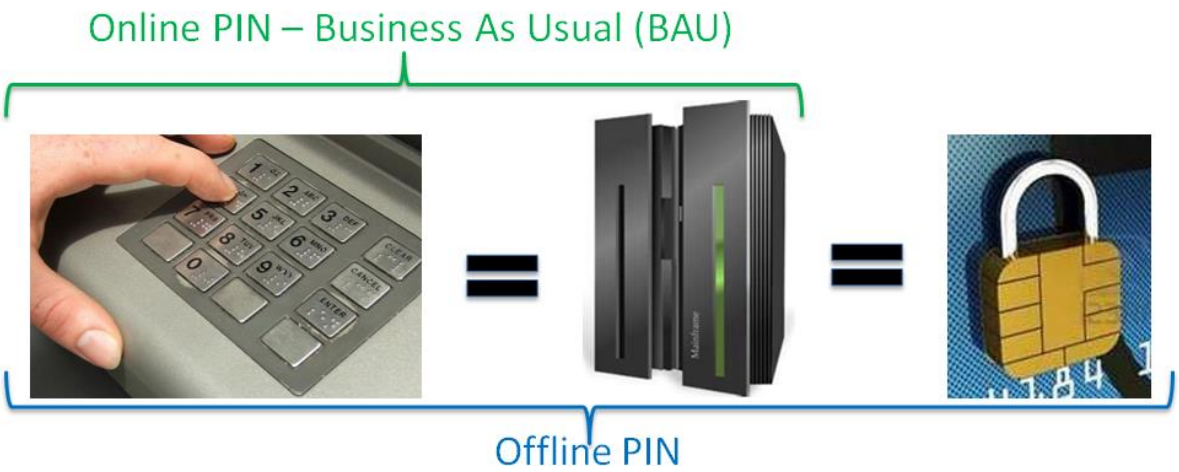


Diagram 3-5: Online PIN vs. Offline PIN

The manner in which the PIN Offset is stored and updated on the host system is the same for a chip card as it is for a magnetic stripe card.

3.6 Managing Offline PIN Tries Within the Chip

When implementing offline PIN, there are some important data elements (EMV tags) that must be stored in the chip in addition to the PIN itself.

The issuer must specify the maximum number of offline PIN tries that are allowed. This indicates how many times the cardholder is allowed to enter a PIN that is determined to be incorrect through the process of offline PIN verification before some other action must be taken. This subsequent action could be, for example, to force the transaction (containing the encrypted PIN) to be sent online to the host for PIN verification and transaction authorization. The appropriate action to take in this situation is indicated in the ICC application as part of card personalization.

Additionally, the chip will contain an offline PIN tries counter that keeps track of how many consecutive failed attempts have been made to verify the offline PIN. When the cardholder enters their PIN and it is verified successfully offline, and the maximum number of offline "bad" PIN tries has not yet been reached, the offline PIN tries counter is automatically reset to indicate that no consecutive bad PIN tries have occurred.

3.7 Unblocking the Offline PIN

When the maximum number of "bad" offline PIN tries has been reached, the offline PIN in the chip is considered "blocked." An issuer whose chip cards support offline PIN verification must provide a way for the offline PIN to be reset, or unblocked. This is typically accomplished by sending a PIN Unblock issuer script to the chip card. The PIN Unblock script is supported by most chip specifications. The following example demonstrates the most common reason for, and use of, the PIN Unblock script.

A chip card is presented at a POS terminal; the chip card and the POS terminal support offline PIN verification, and this is the CVM that is selected by the terminal. The cardholder enters their PIN incorrectly three times in a row (with three being the maximum number of consecutive bad offline PIN tries that are allowed by this issuer). The offline PIN in the card is now blocked, but the cardholder can still perform transactions using another CVM; typically the PIN entered by the cardholder must now be sent online to the host for verification for all transactions until the offline PIN is unblocked; that is, the offline PIN tries counter is reset.

The next time this card is used in an online transaction, one of the EMV tags (Tag 95, TVR) in the transaction request will indicate that the offline PIN try limit has been exceeded. If the PIN in the current transaction is successfully verified, the authorization system may decide to unblock the PIN in the chip, since the cardholder evidently knew their correct PIN. The host will then send a PIN Unblock script with the transaction response. The terminal will pass the script to the chip card, and the chip will attempt to execute the PIN Unblock command. If the command is successfully executed, the offline PIN tries counter in the chip is reset, and offline PIN verification can again be attempted between the card and a POS terminal that supports offline PIN verification.

All of this activity related to the offline PIN should be completely transparent to the cardholder, including whether the PIN is verified offline or online, whether an issuer script is received, and whether the script updates a field in the chip.

A PIN Unblock issuer script can be sent with either an ATM online response or a POS online response. It is up to the issuer to decide whether to send the PIN Unblock script with the next online transaction response (regardless of whether it is ATM or POS), or only send the script with the next online ATM transaction response. Similar considerations for issuers are discussed later in this document.

Some software products support an explicit PIN Unblock transaction at the ATM; however, an ATM owner may or may not want to offer this option to the cardholder. Most cardholders would not understand the purpose of a PIN Unblock transaction; they may assume this function has something to do with their online PIN. This option is inappropriate for a magnetic stripe card, since there is no offline PIN to unblock with a magnetic stripe card. Because the PIN Unblock script only applies to chip cards containing an offline PIN, an explicit PIN Unblock transaction might not be used very often at most ATMs.

4 Current Payment Network Offerings

4.1 American Express

The American Express Global Network Services (AEGNS) Network Specification dated October 2013 supports explicit PIN Change and PIN Unblock through ATM request, response, reversal, and reversal acknowledgement messages. There are unique processing codes for the PIN Change (960000) and the PIN Unblock (970000).

The American Express Integrated Circuit Card Payment Specification (AEIPS), version 4.2 dated June 2011, supports the PIN Change and PIN Unblock issuer scripts. Members must support these issuer scripts if offline PIN is supported.

According to American Express, a partner wishing to implement PIN management must abide by the following business rules:

- Follow PIN Management requirements and message formats in accordance with the AEIPS specification
- Certify with American Express for sending and receiving PIN management-related messages
- Support PIN Change and PIN Unblock
- Handle PINs up to 12 digits in length
- Process post-issuance scripts, including sending error messages if the PIN Change or Unblock was unsuccessful

4.2 Discover

The Discover Network Authorization Interface Technical Specifications, Release 13.2 dated October 18, 2013, supports PIN Change and PIN Unblock transactions.

The Diners Club International Xpress Authorization System ISO 8583 Transaction Manual, version 13.2 dated October 18, 2013, includes support for PIN Change and PIN Unblock transactions.

Both specifications use unique processing codes for the PIN Change (98) and the PIN Unblock (99).

The Discover Payment Application Specification (D-PAS) supports the PIN Change and PIN Unblock issuer scripts.

4.3 MasterCard

The MasterCard Dual Message System (DMS) Customer Interface Specification dated November 13, 2013 includes support for PIN Change and PIN Unblock transactions. There are unique processing codes for the PIN Change (92) and the PIN Unblock (91).

The MasterCard Integrated Processing Solutions (IPS) ISO Specification Guide, Version 7, dated October 2011, includes support for the PIN Change transaction. This specification does not mention PIN Unblock.

The M/Chip 4 v1.1 Card Application Specifications for Debit and Credit dated October 2006 supports the PIN Change and PIN Unblock scripts.

4.4 Visa

Visa does not offer PIN change in the U.S. However, the Visa Base I Technical Specifications, Volume I, December 2011, support unique processing codes (transaction types) for PIN Change (70) and Pin Unblock (72).

4.5 Other Debit Payment Networks

Many other debit payment networks do support PIN change at the ATM. Please refer to the operating rules and interface specifications from the specific networks for more information.

5 Key Decisions for ATM Owners and Issuers

ATM owners and issuers must first make some very basic decisions about if, where, and how to offer PIN Change at the ATM. These decisions may involve discussions with multiple payment networks.

5.1 PIN Change at the ATM: Yes or No

The first decision to make is whether to support PIN Change at the ATM at all.

ATM owners who currently support PIN Change at the ATM for magnetic stripe will most likely want to continue to offer this feature after the introduction of EMV, in order to provide continued service to cardholders who are accustomed to using the feature. It may be difficult to justify discontinuing a feature that customers have come to rely upon.

ATM owners who do not support PIN Change today must decide if they wish to do so, and if so, when, and under what circumstances. Because PIN Change is possibly the most complex EMV transaction, these ATM owners may want to delay implementing this feature until basic EMV functionality has been implemented successfully. Of course, for business reasons, it may not be possible to delay implementation of PIN Change at the ATM; some ATM owners may find that they are tasked with including this feature in their initial EMV migration project. These ATM owners may find that including this feature adds to the timeline and cost of their project, primarily because of the additional states, screens, and configuration required at the ATM and the significant amount of testing required to test not only positive scenarios, but many negative scenarios as well. In addition, changes are needed not only to the ATM, but on the issuer's authorization system as well.

The rest of this section assumes that the ATM owner has decided to move forward with implementing PIN Change at the ATM.

5.2 Card Technology

The ATM owner must decide whether they will offer PIN Change

- For magnetic stripe cards only
- For chip cards only
- For magnetic stripe cards and chip cards

As previously noted, it is usually very difficult to remove a feature that cardholders rely upon, so if the ATM owner already offers PIN Change at the ATM for magnetic stripe cards, they will most likely support it for both magnetic stripe and chip cards. From the ATM's perspective, there is very little difference between a PIN Change for a magnetic stripe card and a PIN Change for a chip card. The additional steps that are needed to support PIN Change for a chip card (reading the chip, passing an issuer script to the chip, and handling unsolicited messages from the chip which result in the creation of a reversal) are also needed for other types of EMV transactions. Therefore, from the ATM perspective, there is usually no

technical reason not to support PIN Change at the ATM for both types of payment cards. There may, however, be business considerations that drive this decision.

5.3 Card and Terminal Technology

ATM owners must also decide whether to support PIN Change:

- Only at magnetic stripe-only ATMs
- Only at EMV-enabled ATMs
- At all ATMs

Consideration must then be given to the resulting combinations of card and terminal technology; for example:

- Magnetic stripe card at magnetic stripe-only ATM
- Chip card at magnetic stripe-only ATM
- Magnetic stripe card at EMV-enabled ATM
- Chip card at EMV-enabled ATM where the chip is read successfully
- Chip card at EMV-enabled ATM where the chip is not read successfully (fallback)

For example, with an ATM that supports magnetic stripe cards only, the ATM owner may not offer PIN change at all, or, if PIN Change is offered, it would be only for magnetic stripe cards.

A more challenging situation is where the ATM supports magnetic stripe and chip. When presented with a magnetic stripe card, will the ATM offer PIN change at all, or only for magnetic stripe cards? When presented with a chip card, will the ATM offer PIN change at all, only for magnetic stripe, or for magnetic stripe and chip cards?

5.4 PIN Change Scope

The ATM owner must also decide the circumstances under which they will offer PIN change to cardholders:

- On-us only
- In-network; if so, which network(s)?
- Not-in-network (regional, domestic, or unrestricted)

This is usually more of a business decision than a technical decision, since the steps required for the transaction do not vary much based on the decision. Updates to Financial Institution Tables (FIT) or similar logic are typically sufficient to determine when the PIN Change option will be presented to the cardholder. For example, PIN Change might be offered only to cards using specific BINs.

5.5 ATM Loads

As noted in Section 4, the values used for transaction/processing codes for PIN Change and PIN Unblock are not consistent across the payment networks. This may not be a problem if the ATM owner supports PIN Change on-us only. However, if ATMs are to support PIN Change within a specific network, load files cannot be generic. When the customer selects PIN Change, the ATM must be able to determine the card scheme/payment network (or RID) and the associated PIN Change transaction/processing code. Changes to state flow will be needed for those supporting older technology. Those with stateless ATMs must find a way to associate the appropriate transaction/processing code to the PIN Change transaction.

5.6 Special Scenarios

In addition to the decisions above, ATM owners and issuers need to determine how they will handle some special scenarios. Each scenario must be thoroughly tested, which is not always possible using a "real" ATM. Simulators are essential in order to test all combinations of card technology, terminal technology, functions, faults, and other features at the ATM, not just PIN Change.

5.6.1 Fallback

Technical fallback, or simply fallback, refers to the scenario where a chip card is presented to a chip-enabled terminal, but for some reason the chip cannot be read. There are legitimate situations which may cause this to occur; for example, the chip has been damaged, or the chip reader contacts are dirty and cannot make good contact with the chip on the card. But fallback can also indicate fraud. For example, if the Track 2 data was skimmed from a legitimate chip card and placed onto a blank white plastic (counterfeit) card, the service code in the Track 2 data indicates the presence of a chip, but the chip reader cannot read a chip, since one is not present.

Payment networks often have international and regional requirements as to how fallback is to be handled at the payment terminal. These requirements must be followed by ATM owners. In addition, some countries have developed best practices about how fallback "should" be handled at the payment terminal. Refer to Section 7.1 in the EMV Migration Forum's white paper "Implementing EMV at the ATM: Requirements and Recommendations for the U.S. ATM Community" for more information on fallback.

The ATM does not know if a chip card supports offline PIN verification or not. Fallback for a PIN Change transaction therefore presents a very interesting challenge.

If the card supports online PIN only, the PIN Change transaction could theoretically proceed as follows:

- The magnetic stripe fallback transaction request would indicate PIN Change and would contain the current PIN (encrypted) and the new PIN (encrypted)
- The host should recognize that this card does not support offline PIN. The host can verify the current PIN, generate the PIN Offset for the new PIN, store the new PIN Offset, and generate a

transaction response indicating the PIN Change was approved. The host will not need to send an issuer script.

- The ATM will receive the response and display a message to the cardholder that the PIN Change was successful.

However, if the chip supports offline PIN Change, but the chip reader cannot communicate with the chip (hence the fallback transaction), any issuer script from the host will not be delivered to the chip. This would result in an out-of-sync condition, where the PIN Offset on the host does not reflect the same PIN that is in the chip.

The host should be able to determine, based on information in the transaction request, that the chip could not be read. If the host can also determine that the card supports offline PIN, the issuer can decline the PIN Change transaction. Problems such as the out-of-sync condition arise if the host cannot detect fallback, or determine that the card supports offline PIN, and the host approves the transactions and sends the PIN Change issuer script anyway. It is therefore vital that the host system be able to detect this situation when supporting offline PIN management. But it is possible that the host may not take the correct action; for example, the host may send an issuer script for a fallback transaction.

ATM owners must pay special attention to combinations of card and terminal technology, and situations such as fallback, to determine whether to allow functions such as PIN Change in each situation.

Special considerations for issuers are discussed later in this document.

5.6.2 Chip Card at Magnetic-Stripe Only ATM

Although the discussion above focuses on fallback, similar situations can arise when a chip card is presented to a magnetic stripe-only ATM. This ATM cannot read the chip, so the ATM has no idea whether the chip supports offline PIN or not. This ATM also cannot deliver an issuer script to the chip.

ATM owners may elect to accept a PIN Change transaction request in this scenario, and hope that the issuer will

- Detect the combination of card and terminal technology
- Know whether the card supports offline PIN or not
- Only send a PIN Change issuer script when the card supports offline PIN ***and*** the transaction was initiated at an EMV-enabled ATM ***and*** the chip was read successfully
- Approve or decline the transaction accordingly

ATM owners may instead decide not to allow PIN Change for chip cards at magnetic stripe-only ATMs. This would avoid problems that may result when an issuer does not handle these situations correctly.

5.6.3 Out of Sync Conditions

In a complex transaction such as PIN Change, there is always the possibility that something does not go as planned. For example:

- A chip card containing an offline PIN performs a PIN Change at a chip-enabled ATM; the issuer approves the PIN Change and sends an issuer script to the ATM, but the issuer script is not delivered to chip; this could be due to a hardware malfunction at the ATM
- A chip card containing an offline PIN performs a PIN Change at a chip-enabled ATM; the issuer approves the PIN Change, the issuer script is delivered to the chip, but the PIN change command is not executed by chip. This can happen for one of any number of reasons, for example:
  - The issuer script or embedded PIN Change command is formatted incorrectly
  - The chip cannot decrypt the new PIN

In either scenario, the host assumes the PIN Change transaction will complete normally when the response reaches the ATM, so the PIN Offset on the host has been updated to reflect the new PIN. But the PIN in the chip is not changed, so an “out of sync” condition results.

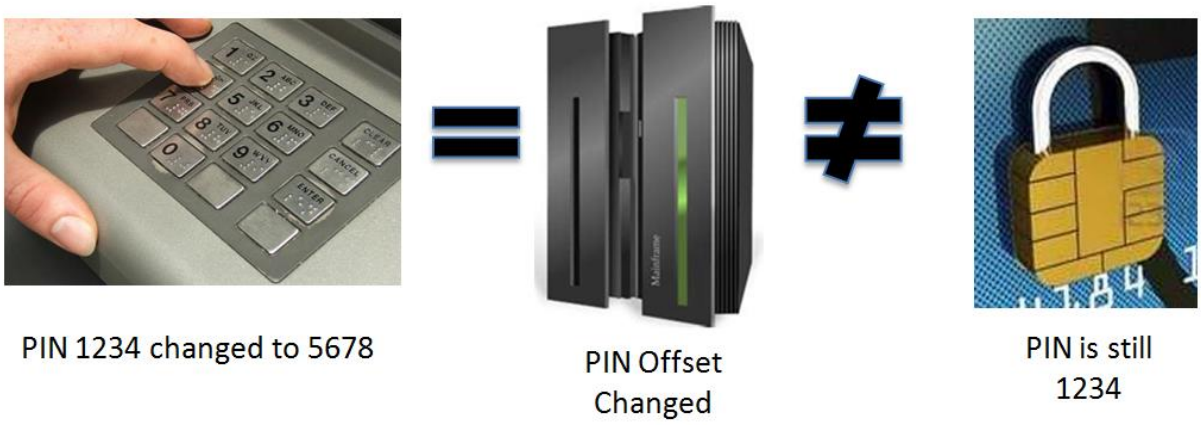


Diagram 3-5: Out of Sync Condition

This out of sync condition must be corrected as soon as possible. If it is not corrected, and the cardholder attempts to use their card at a POS terminal that supports offline PIN verification, the cardholder will believe they have changed their PIN and will enter their new PIN, which cannot be successfully verified against the “old” PIN that is still in the chip. If a transaction containing the encrypted (new) PIN would go online, however, the new PIN would be verified successfully. If the transaction cannot go online (for example, if the merchant’s link to the acquirer is down), but requires PIN verification, the transaction cannot complete successfully.

If the chip receives a PIN Change issuer script, and the chip cannot execute the embedded PIN Change command, the chip will send an unsolicited status message to the terminal with a status code that indicates the command was not executed successfully. The terminal must generate a reversal in this

situation, so that the issuer knows the PIN in the chip was not changed. The issuer must then revert back to the value of the PIN Offset prior to the PIN Change transaction.

It is important to note that PIN Change is the only scenario where the issuer must be notified immediately if a command in the issuer script is not executed. The issuer will be notified in the next online transaction request (initiated by the same card at an ATM or POS terminal) about the failure to execute any issuer script, but failure to execute the PIN Change command is considered serious, due to the possibility of problems with subsequent transactions; therefore the issuer must also be notified immediately.

Note that, depending on the technology employed by the ATM, if the PIN Change issuer script is not executed, and the chip card sends an unsolicited status to the ATM as a result, the ATM may send a solicited status to the acquirer host indicating that the transaction has failed. If the acquirer and the issuer are the same entity (i.e., this is an on-us transaction), the PIN Offset can be rolled back immediately by the host. If the acquirer and the issuer are not the same entity (i.e., this is a not-on-us transaction), the acquirer host must format a reversal and deliver it to the appropriate destination.

Regardless of whether the reversal is formatted by the ATM or the acquirer host, an immediate reversal to the issuer is essential in this scenario.

5.6.4 Failure to Execute the PIN Change Command in an Issuer Script

If the chip card receives an issuer script containing a PIN Change command, but the PIN Change command cannot be executed, the chip will send an unsolicited status message to the ATM. This message is considered unsolicited, because the ATM assumed that the transaction was finished when the issuer script was passed to the chip. ATM owners must test this scenario to ensure that the ATM recognizes it, and that the ATM (or the acquiring host) will generate and send a reversal message to the issuer.

The issuer must then “back out” the new PIN Offset and replace it with the PIN Offset associated with the previous PIN. Obviously, the issuer must be able to determine the PIN Offset for the previous PIN; this can create issues since some systems do not maintain information about the previous PIN.

Some network specifications may carry the previous PIN Offset or the previous encrypted PIN in the reversal message, and others may not. Issuers must become familiar with the network specifications relevant to their organization, and understand the potential impacts to their host system for information that is, or is not, provided in this situation. Issuers will then be able to determine whether any changes must be made to their host system to store both the current and the previous PIN Offset.

6 Additional Considerations for ATM Owners

ATM owners who support PIN Change at the ATM for magnetic stripe will most likely want to continue to offer this feature after the introduction of EMV, to provide continued service to cardholders who are accustomed to using the feature.

Once the ATM has been upgraded to support basic EMV functions, very few (if any) additional software or configuration changes may be needed to support PIN Change for chip cards. Issuer scripts are not unique to PIN Change; ATMs must be able to pass issuer scripts to a chip card in order to pass terminal certification, regardless of the commands contained within an issuer script.

The ATM will need to support the following for any EMV transaction, including PIN Change:

- Distinguish between on-us, in-network, and not-in-network scenarios (depending on business requirements)
- Distinguish between magnetic stripe cards and chip cards
- Present functions appropriate for the combination of card and terminal technology
- Present functions appropriate for business requirements (e.g., PIN Change may be allowed on-us only)
- Present appropriate verbiage on customer-facing screens
- Pass issuer scripts to cards
- Handle unsolicited messages and reversal situations

An ATM owner who has not previously offered PIN Change at the ATM, but decides to implement this feature, must add the specific configuration, screen flow, messages to cardholders, and other functions that are required to support this feature. PIN Change-specific items may include:

- Modifications to the FIT table to indicate when and for whom the PIN Change function is offered
- Recognizing card technology being presented (magnetic stripe or chip) and displaying PIN Change for appropriate technology (if only offering PIN Change for one technology)
- New states and screens to support the first entry of the new PIN and second (confirmation) entry of the new PIN
- Messages to the cardholder prompting them what to do next

Extensive testing will be required.

The actual flow of states, screens, and cardholder-facing messages may vary slightly, depending on whether the ATM is configured to read the magnetic stripe before reading the chip, or vice versa. As noted in Section 2.7 in the main body of the white paper "Implementing EMV at the ATM: Requirements and Recommendations for the U.S. ATM Community", it is likely that U.S. ATMs will initially be configured to read the magnetic stripe first; then, if so indicated by the service code in the Track 2, attempt to read the chip. This may change in the future, when EMV reaches critical mass in the U.S. and there are significantly more chip cards than magnetic stripe cards in production.

Several levels of EMV certifications must be executed before moving an EMV-enabled ATM into production. These certifications typically include tests with issuer scripts. ATM owners can request a waiver from the relevant payment network for any test that represents a function that the ATM owner does not support.

As previously noted, ATM owners need to pay special attention to the possible combinations of card and terminal technology, and decide which functions to allow for each combination.

ATM owners who use monitoring tools will find that their software may emit new log messages for EMV. These log messages may include specific messages related to PIN Change.

ATM owners should be aware that adding PIN Change at the ATM is a complex function, which will increase project time and the amount of testing that is required for ATMs and online transaction processing software. If possible, ATM owners who do not support PIN Change at the ATM today should consider implementing PIN Change at the ATM as a subsequent phase of their EMV migration project, once basic EMV functionality is stable and working as expected.

7 Additional Considerations for Issuers

The effort to implement PIN Change is not restricted to ATM owners. Clearly, there is an impact to issuers as well.

This section presents considerations relevant to issuers regarding PIN Change at the ATM.

7.1 Supporting Offline PIN Verification

Supporting offline PIN verification in a chip card is not mandatory, and is also unnecessary for cards that will only be used at ATMs, since ATMs cannot support offline PIN verification. An issuer may decide it is too costly and time-consuming to support offline PIN verification in their chip cards, especially if U.S. POS terminals do not support it. In order to make an informed decision about whether or not to support offline PIN verification in their chip cards, issuers must consider where and how their chip cards will be used. As an example, an issuer might decide that only the chip cards in certain portfolios will support offline PIN verification, for example:

- Corporate cards
- Cards for international travelers
- Only chip cards with applications that can be used at a POS device
- Only credit cards

Cards that support both online and offline PIN provide a positive experience for international travelers, since many international implementations of EMV use offline PIN.

Issuers need to be aware that cards with offline PIN verification support may cost more than cards without offline PIN verification support, due to requirements for additional memory (to house additional EMV Tags, keys, and certificates) and stronger cryptography (to support public key infrastructure for offline enciphered PINs).

Cards with offline PIN verification support must undergo additional quality assurance testing, to ensure that the offline PIN, and related EMV tags, are managed properly, and that issuer scripts are executed appropriately. An EMV migration project for an issuer is therefore more complex, time-consuming, and expensive when supporting offline PIN verification than an implementation that requires only online PIN verification.

Very few cardholders would understand the difference between an online PIN and an offline PIN. Therefore, although it is technically possible to assign a unique PIN to each ICC application on a chip card, issuers typically configure a chip card so that the same PIN is used by all applications on the card that require a PIN.

7.2 Authorization Logic

Issuers will need to assess the steps taken by their authorization system to ensure that they are utilizing EMV data to its fullest potential. There are several fields in an online transaction request that can tell an issuer a lot about what actually happened at the terminal, not just for PIN Change transactions, but all online transactions. Some examples are presented below.

7.2.1 Point of Service Data Code (also known as the Point of Service Entry Mode)

This field typically contains twelve subfields. Those that are of particular importance in this discussion are:

Card Data Input Capability: indicates the primary way in which the terminal can accept data from the card. Magnetic stripe-only terminals will have a value of 2 in this subfield. If the terminal is EMV-enabled, there will be a value of 5 in this field (even if the terminal also supports magnetic stripe).

Card Data Input Mode: indicates how the terminal actually obtained data from the card. If the magnetic stripe was read, there will be a value of 2 in this subfield. If the chip was successfully read, there will be a value of 5 in this field.

7.2.2 Track 2

The Track 2 from the magnetic stripe has a specific format. An EMV tag in the chip (Tag 57) contains the Track 2 equivalent data, which is slightly different from the Track 2 in the magnetic stripe. If the magnetic stripe data is used for the transaction, the Track 2 data from the magnetic stripe will be found in the online transaction request. If the chip is successfully read, then the data from EMV Tag 57 will be found in the online transaction request.

The Service Code appears in the Track 2 of the magnetic stripe and in EMV Tag 57. As described in Section 2.7 in the main body of the white paper "Implementing EMV at the ATM: Requirements and Recommendations for the U.S. ATM Community," the first digit of the service code indicates whether the card was created as a magnetic stripe card or a chip card.

7.2.3 Authorization Request Cryptogram (ARQC)

If the chip was successfully read, it should generate an ARQC for an online transaction request. If there is no ARQC in the online transaction request, this usually means the magnetic stripe was read (either because the card had no chip, or because the chip could not be read).

7.2.4 Terminal Verification Results (TVR)

EMV Tag 95 (TVR) contains a lot of useful information about what happened at the terminal, from the terminal's perspective. For more information about the TVR, refer to the EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 3, Annex C5.

7.2.5 Card Verification Results (CVR)

The CVR includes information for the issuer regarding the results of card risk management processing and application processing. The CVR is typically found in the Issuer Application Data, or IAD (EMV Tag 9F10) in the transaction request. The format of the IAD may vary slightly from one network specification to another. The CVR contains, among other things:

- An indication of how many issuer scripts were successfully processed by the chip during the previous online transaction. If an issuer script was not processed, the host may wish to resend it.
- Whether the offline bad PIN try limit has been exceeded. In this case, the issuer may wish to send a PIN Unblock script. Additional information on this topic is included in Section 7.4 below.

7.2.6 Examples

Analysis of the fields described above is critical in order to detect potential fraudulent situations as well as situations where there is a legitimate problem in the chip or the terminal. The transaction authorization logic on the host system should take into consideration combinations of data that are invalid or unusual. Fraud detection systems may automatically “learn” these combinations, or specific rules can be created to look for them.

For example, the following combination usually indicates fallback:

- The first digit of the Service Code indicates that the card was created as a chip card
- The Card Data Input Capability indicates that the terminal is EMV-enabled
- The Card Data Input Mode indicates that the magnetic stripe was read
- No ARQC is present

Some network specifications even have specific values in other fields that indicate potential fallback.

Using another example, the following combination usually indicates that a chip card was used at a terminal that is not EMV-enabled:

- The first digit of the Service Code indicates that the card was created as a chip card
- The Card Data Input Capability indicates that the terminal is not EMV-enabled
- The Card Data Input Mode indicates that the magnetic stripe was read
- No ARQC is present

7.3 Tracking Bad PIN Tries

If a chip card supports offline PIN verification, the offline bad PIN tries are tracked in the chip. Issuers may already be familiar with the online bad PIN tries counter, which is maintained on the host. These two values do not necessarily work in conjunction with each other.

As an example, assume the offline bad PIN tries limit in the chip is set to 3, and the online bad PIN tries limit is also set to 3, for a chip card that supports offline PIN verification. The cardholder uses the card at a POS terminal that supports offline PIN verification. The cardholder enters their PIN incorrectly three times, so the offline PIN tries on the card has reached its limit, and the offline PIN is now blocked. Assume that the card is programmed so that when this happens, the transaction, containing the encrypted PIN, must go online so that the PIN can be verified by the host. The cardholder enters their PIN wrong three more times at the POS terminal, or the cardholder enters the PIN wrong three times at an ATM. In either case, the transaction goes online with the incorrect PIN, so the online bad PIN tries is now at its limit.

An issuer may initially wonder why the cardholder was allowed a total of six bad PIN tries. The chip is tracking the offline bad PIN tries, and the host is tracking the online bad PIN tries, and the two counters usually do not work in conjunction with one another; that is, when one counter reaches its limit, the other counter is most likely unaware of it.

7.4 When to Deliver PIN Change and PIN Unblock Issuer Scripts

As noted previously in this document, when the offline PIN is blocked, a bit in EMV Tag 95 (TVR) is set in the next online transaction request. This field should never be set if the card does not support offline PIN verification.

If the offline PIN is blocked, the issuer can send a PIN Unblock script to the card as part of the online transaction response. However, the issuer will probably not want to do this unless the PIN in the current online transaction request is verified successfully. In addition, the issuer must determine whether they will send issuer scripts with ATM and POS transaction responses, or only with ATM transaction responses. If the current transaction was initiated at a POS terminal, and the issuer only wants to send issuer scripts with ATM transaction responses, the host system must wait to send the PIN Unblock issuer script to the card until the next online ATM transaction is initiated by that card where the online PIN is verified successfully.

If the offline (or online) bad PIN tries limit is exceeded frequently, the issuer may wish to contact the cardholder and make sure the card was not lost or stolen, or there is some other problem.

7.5 Stand-In Scenarios

In order to support basic EMV functions such as verifying the ARQC and generating the ARPC, the HSM must support the appropriate EMV extensions and commands. Supporting offline PIN management may require additional HSM commands.

If an issuer is unable to upgrade their host system (specifically the online transaction authorization logic) to verify the ARQC, generate the ARPC, and analyze the EMV data as described above, the issuer may have these functions performed by a processor or network on their behalf. Even if the issuer is able to perform these functions, the issuer may have arrangements with a processor or network to "stand in" for them when their host system is unavailable. Issuers must decide what EMV functions they want the "on behalf of" (OBO) party to perform on their behalf, and which functions may be considered too sensitive to be performed by the OBO party. For example, the issuer may not want the OBO party to handle PIN Change; the issuer would ask the OBO party to decline any PIN Change requests that are received while the issuer's host system is down.

If the issuer is unable to perform the most basic EMV functions such as verifying and generating cryptograms, then supporting offline PIN management, PIN Change and PIN Unblock scripts may not be feasible. The issuer will need to decide if they want the OBO party to perform these functions.

8 Conclusion

Key points that ATM owners and/or issuers may wish to consider in connection with the U.S. EMV migration include the following:

- ATMs operate in an "online only" environment; this does not change with the introduction of EMV.
- If a magnetic stripe card or a chip card is to be used at an ATM, the card must support online PIN verification.
- PIN Change at the ATM is offered as a convenience for the cardholder. The ATM is also a convenient way to deliver issuer scripts, including PIN Change and PIN Unblock, to a chip card.
- Supporting PIN Change at U.S. ATMs is not mandated by EMVCo or any of the payment networks at this time. (In Europe, MasterCard strongly recommends support for PIN management (PIN Change and PIN Unblock) due to the high use of offline PIN verification in that region.)
- If PIN Change is to be supported at the ATM, the PIN Offset must be stored on the host.
- If the chip card supports offline PIN verification, the PIN must be stored in the chip.
- If the chip card does not support offline PIN verification, the PIN is not stored in the chip.
- If the chip card supports both online PIN verification and offline PIN verification
    - The PIN Offset must be stored on the host, and
    - The PIN must be stored in the chip
- The PIN in the chip and the PIN Offset stored on the host must be synchronized in order to facilitate online (ATM or POS) and offline (POS) transactions that require a PIN.
- When supporting offline PIN management, the issuer's host system must be able to unblock the offline PIN in the chip by sending a PIN Unblock script under the appropriate conditions.
- Issuers will need to make sure the authorization system can detect fallback and other potential problem scenarios that may occur for various combinations of card and terminal technology.
- ATM owners and issuers have many decisions to make regarding if, how, where, and when to implement PIN Change at the ATM.

Offline PIN management is one of the most complex functions of EMV. The "normal" scenario, where the PIN Change transaction functions as expected, takes a significant amount of time to test and verify. Negative testing and reversals add complexity. When multiple parties are involved, it is even more complex and challenging. The amount of testing that is required cannot be overstated. ATM owners and issuers who do not offer PIN Change at the ATM today may want to consider first ensuring that basic EMV functionality is implemented successfully, before adding support for PIN Change at the ATM.

Whatever the U.S. payments industry, or an individual stakeholder, decides to do regarding PIN Change at the ATM, all stakeholders should remember how important it is for the consumer to have a consistent and positive experience. Each stakeholder's EMV migration project can be a great success, but it also has many potential points of failure. PIN Change by a chip card at a chip-enabled ATM offers more potential points of failure than any other EMV transaction. With the immediacy of communications through social

media and the Internet, when a consumer has a bad experience, millions of people can be aware of it within minutes. It is critically important to make wise business and technical decisions, plan carefully, and test thoroughly, to ensure that EMV migration projects are successful.

9 Publication Acknowledgements

This document 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 PIN Change at the ATM in the United States.

Publication of this document by the EMV Migration Forum does not imply the endorsement of any of the member organizations of the Forum.

The EMV Migration Forum thanks **Deborah Spidle**, Paragon Application Systems, and **Marc Cleven**, Visa, for leading the project and for writing the content for this document. The EMV Migration Forum wishes to thank the ATM Working Committee members for their contributions and review of this document.

Trademark Notice

10 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).

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 digits 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., DNA, 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 hexadecimal 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.