
# Introduction to EMV Chip & PIN

# Table of Contents

# Chapter 1 - Introduction

This document provides an introduction to EMV Chip & PIN migration.

It explains Chip & PIN and how it works; provides a brief description of the hardware involved; outlines the timescales for Chip & PIN adoption; and describes fallback procedures. A diagram illustrates the message flow for a Chip & PIN transaction.

This document also includes a section on EMV migration, explaining what EMV migration is, the timescales involved and who is responsible for overseeing it.

Finally, there is a list of frequently asked questions for Chip & PIN and EMV.

# Chapter 2 - Chip & PIN and its Benefits

## 2.1 What is Chip & PIN?

Chip & PIN is a secure card payment system to help prevent fraud. The chip is intended to ensure that the card is authentic and the PIN ensures that the cardholder is genuine.

## 2.2 Chip

The 'chip' part refers to the smart card – a plastic payment card with an embedded microprocessor. The chip contains the same information as a magnetic stripe but it also has additional processing capabilities and a secure memory. The microprocessor can also hold multiple applications, where an application may be a specific brand of credit card, a loyalty card, gift card, staff discount card, etc; so a cardholder could have credit and debit applications, loyalty applications and electronic ticketing on a single physical card. One chip can hold the information from several magnetic stripes and the chip holds information so securely that it is very difficult to copy or alter it, unlike the magnetic stripe.

Chip cards are already being issued to cardholders, but they only contain a basic credit or debit application and they are currently swiped through a magnetic stripe reader; they do not support PIN verification. Therefore, issuing banks must send new PIN-enabled chip cards to all cardholders within the next two years. In addition, retailers must replace or upgrade their PoS equipment and all ATMs must be replaced or converted so that they can accept chip cards.

## 2.3 PIN

The 'PIN' part refers to the Personal Identification Number – a 4-digit number that cardholders use to identify themselves instead of signing a receipt (the PIN may be longer than 4 digits for non-UK users). This can be the same as the PIN that the cardholder uses at an ATM when withdrawing cash. When the cardholder hands over their card to pay for a purchase, instead of being asked for their signature, they will be asked to type their PIN into a PIN pad.

The PIN entered by the cardholder is either checked by the card itself against the PIN that is stored, securely encrypted, on the card, or it is encrypted and sent to the acquirer in the online authorisation request message. These methods are known as 'offline PIN verification' and 'online PIN verification' (see below).

The PIN is only used in a customer-present situation and authorisation will only occur once the cardholder has entered the correct PIN. A cardholder will not use a PIN in an Internet or telephone transaction, as this would mean disclosing the PIN to a third party.

## 2.4 Offline PIN Verification

Offline PIN verification means that the PIN can be verified without going online to the acquiring bank. With offline PIN verification, the PIN that the cardholder enters is checked by the card itself. This will save time at the till because the transaction does not need to go online to check the cardholder's identity.

## 2.5 Online PIN Verification

The issuer performs online PIN verification. The PIN entered by the cardholder into the PIN pad is securely encrypted and sent from the terminal to the acquirer in the authorisation request message. This method can be used for both magnetic-stripe and chip card transactions. The card itself can decide to force online PIN verification under certain circumstances. For example, if the pattern of card use is unusual, the card may force online PIN verification to ensure that it is not being used fraudulently. This method can also be used to facilitate cash withdrawal at the Point of Sale.

## 2.6 PIN Pad

The cardholder uses a PIN pad to choose which application they want to use for a transaction and to enter their PIN.

The PIN pad might take a number of forms, such as:

- A separate device attached to the till by a cable, which can be passed to the cardholder
- A combined card reader and PIN pad, where the cardholder can insert their card then enter their PIN
- A device built into the shop counter
- A portable device, not connected to the till; this may be used in a restaurant, where the waiter will take it to the customer at the table. This avoids the danger of skimming when the card is taken out of the customer's view.

## 2.7 Locked Cards

If a cardholder enters their PIN incorrectly three times in a row, the card will be locked and they must use an alternative means of payment for that transaction. The card must then be unlocked at an ATM. If the cardholder cannot remember their PIN, they must contact his issuing bank, which will either re-advise the cardholder of their PIN or issue a new one. Once this has been done, the cardholder must then unlock the PIN at an ATM. A cardholder can change their PIN at an ATM at any time.

## 2.8 Fallback

There will be a period of transition following the adoption of PIN verification, during which cardholders will be able to use a signature if they forget their PIN. However, once the transition period is over, if a

cardholder forgets their PIN, they will have to use an alternative means of payment for that transaction.

The magnetic stripe and signature strip will remain on chip cards for several years so that the card can still be used in countries that have not yet adopted Chip & PIN. It also means that during the transition period, if the chip fails during a transaction, a fallback to magnetic stripe and signature is permitted, although it is likely that the transaction will go on-line for authorisation, regardless of the transaction amount. However, after the liability shift date cardholders who have been issued with a PIN-enabled chip card must use PIN for PoS transactions and if the chip cannot be read, the transaction will be terminated.

## 2.9 The Benefits of Chip & PIN

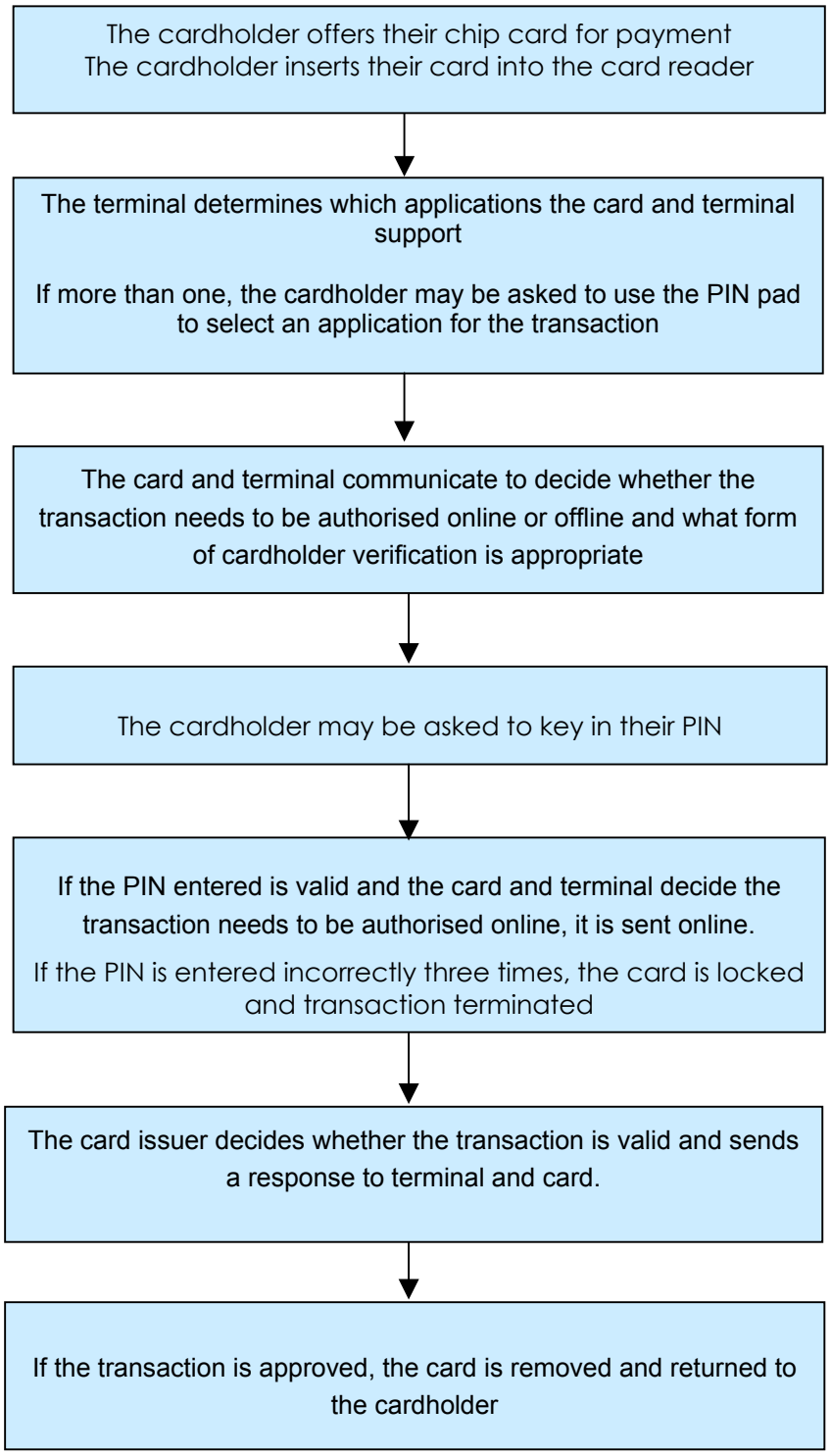
The benefits of Chip & PIN are both short term and long term, including:

- ✓ The process of migrating to EMV Chip & PIN entails the liability for fraud shifting from the banks to merchants who have not adopted Chip & PIN creating a penalty for those merchants. In addition, Merchants that have not adopted Chip & PIN will find themselves increasingly being targeted for fraud. See section 4.5 for more details.
- ✓ Improved security – the data on the chip is extremely difficult to copy or change.
- ✓ Faster transactions at the till – entering a PIN is faster than signing a receipt
- ✓ Fraud costs will be cut for the merchant, including chargebacks and administration costs.
- ✓ The merchant no longer has to keep piles of old receipts
- ✓ The task of identifying the cardholder shifts from the merchant to the card itself
- ✓ Many different applications can be stored on a single card, such as loyalty applications and electronic purse
- ✓ Unattended payment devices can be developed, such as self-scanning and self-service petrol pumps
- ✓ Cardholders are increasingly able to use chip cards to make secure purchases through interactive television, mobile phones and PCs

## 2.10 Drawbacks of Chip & PIN

The drawbacks of Chip & PIN are generally short term and the required investment is likely to be offset by the benefits.

# Chapter 3 - Message Flow for a Chip & PIN Transaction



# Chapter 4 - EMV Migration

## 4.1 What is EMV Migration?

EMV migration is the transition from magnetic stripe credit and debit cards to chip cards.

The banks already have major programmes in place to issue the new chip cards to their cardholders; when purchasing goods, these smart-based cards will also allow cardholders to enter a PIN number, rather than signing a receipt, which will dramatically reduce levels of fraud associated with card payments.

Merchants will need to upgrade their PoS environments. For example, checkouts will need card readers and PIN pads that are capable of accepting and processing these new smart cards. The ATM (Automated Teller Machine) networks are also being upgraded to allow cardholders to change their PIN.

This migration is being overseen by EMVCo (http://www.emvco.com/).

## 4.2 Who is EMVCo?

EMVCo was formed in 1999 by Europay International, MasterCard International and Visa International in order to maintain and develop the EMV ICC Specifications for Payment Systems. These specifications have been developed to ensure 'global interoperability' - so that any EMV-accredited card can be accepted at any EMV-accredited point of sale anywhere in the world.

## 4.3 The EMV Specifications

The EMV specifications are based on the existing standard for integrated circuit cards with contacts (ISO 7816) and are expected to become a global standard. The UK is the first major implementation of this standard.

EMVCo is controlled by a Board of Managers, which has established a number of working groups, currently covering 'card and terminal', 'security' and 'type approval'. These working groups are made up of representatives from Europay, MasterCard and Visa.

## 4.4 Type Approval

One of these working groups is responsible for type approval, a process that defines requirements for testing that terminals comply with the EMV specifications.

EMV-accredited products are approved by EMVCo after undergoing a series of stringent tests. Further approvals are required from American Express, JCB and the acquiring bank before a retailer can accept live transactions.

The EMV test requirements cover two levels:

- Level 1 tests the terminal to chip interface: the electrical and mechanical aspects of a device.

- Level 2 tests the payment application: the transaction processing software, transmission of data and certain security aspects of a device to ensure that the application has the functionality required to support chip transactions.[1]

[1] PIN pads must also comply with other standards, such as those issued by Visa and APACS in the UK. The APACS PIN Entry Device (PED) Guidelines, for example, define the size and design of the device, its method of connection to the main PoS device, security requirements and supported card types.

Testing is carried out by EMV-accredited laboratories. Once a terminal or application has been approved, EMVCo issues a Letter of Approval. A range of terminal types can be tested, including emerging technologies, such as mobile phones, set-top boxes and unattended payment terminals.

## 4.5 The Solution

It is essential that retailers choose a solution provider with extensive experience of the standards, tests and practical implications for implementing EMV in the diverse retail environments in order to ensure a smooth migration.

The Logic Group has an unparalleled level of skill and expertise in retail EMV smart card solutions. We were the World's first organisation to achieve EMV accreditation for an integrated retail system. Since then, The Logic Group has worked with major retailers to architect EMV solutions into the point of sale and central systems infrastructure. We share our knowledge and expertise with leading acquiring banks, enabling a smooth retailer implementation and have worked closely with the card schemes to ensure the practical issues facing retailers are considered as they develop their standards and testing procedures. The Logic Group is ideally placed to help retailers implement highly effective solutions.

# Chapter 5 - EMV Chip & PIN– Frequently Asked Questions

## 5.1 What is Chip & PIN?

Chip & PIN is a secure card payment system to help prevent fraud. The chip ensures that the card is authentic and the PIN ensures that the cardholder is genuine.

The 'chip' refers to the smart card – a plastic payment card with an embedded microprocessor. The chip holds information securely so that it is difficult to copy or alter it.

The 'PIN' is the Personal Identification Number – a 4-digit number that cardholders use to identify themselves instead of signing a receipt.

## 5.2 Why is Chip & PIN being introduced?

Payment card fraud is increasing rapidly; for example, in the UK it has reached over £500 million. This increase in payment card fraud is not sustainable.

Chip & PIN will reduce payment card fraud. Information is held securely on the card and a transaction cannot be completed at the point of sale if the cardholder does not know the correct PIN. The introduction of PIN verification in France led to an 80% cut in point of sale fraud from lost and stolen credit and debit cards.

## 5.3 Will cardholders be able to use Chip & PIN cards abroad?

Chip & PIN programme will be adopted across the world so that cardholders will be able to use their Chip & PIN cards abroad. However, Chip & PIN cards will retain a magnetic stripe and signature strip for a number of years, enabling them to be used in non-EMV compliant countries.

## 5.4 How will a Chip & PIN transaction work?

A Chip & PIN transaction will work exactly like a current transaction but instead of supplying a signature, the cardholder will be asked to type their 4-digit PIN into a PIN pad.

In addition, a chip card can hold a number of different applications, so the cardholder may be asked to select a particular application to use for the transaction. This may also be done using the PIN pad. (An application on a smart card can be a specific brand or credit card or debit card, a loyalty card, staff discount card, etc.)

## 5.5 Can cardholders use their existing cards?

Cardholders can use their existing cards for chip and signature transactions but not for Chip & PIN transactions as the chip cards that are currently in circulation do not support PIN verification at the point of sale. Card issuers will have to replace all cards with PIN-capable chip cards.

## 5.6 How will a cardholder know what his PIN is?

The cardholder's issuing bank will let them know what their PIN is in the same way they do now.

## 5.7 Can a PIN be changed?

Yes. A cardholder can change their PIN at an ATM in the same way they can now.

## 5.8 What happens if a cardholder forgets their PIN?

The cardholder must speak to their issuing bank. They will either be re-advised of their PIN or the bank will issue them with a new one. If a cardholder forgets their PIN at the point of sale, they may be able to use signature instead for a short time following the adoption of PIN verification, but after that, they will need to use an alternative means of payment.

If a cardholder enters the wrong PIN three times in a row, their card will be locked. They will need to use an alternative means of payment for the current transaction and then unlock their card at an ATM.

## 5.9 What is offline PIN?

Offline PIN verification means that the PIN can be verified without going online to the acquiring bank. With offline PIN verification, the PIN that the cardholder enters is checked by the card itself and saves time at the till.

## 5.10 How does a cardholder get a chip card?

The cardholder's issuing bank will send them a PIN-enabled chip card when their current card expires. If their current card does not expire until after the 2005 deadline, they will be issued with a replacement card before their old card expires.

## 5.11 What is the timescale for rollout?

Cardholders' existing credit and debit cards will be replaced with Chip & PIN cards as they expire. This is a gradual process, which is expected to culminate at the end of December 2005. The aim is that, by January 2005, all point of sale transactions will be verified by PIN.

## 5.12 What fallback procedures are there if the chip cannot be read?

There will be an initial transition period following the implementation of PIN, during which time if a chip cannot be read, a fallback to magnetic stripe and signature is permitted, although the transaction will probably be forced online for authorisation, regardless of the transaction amount.

This transition period is likely to last until 31 December 2006, after which time, if a chip cannot be read, the transaction must be terminated.

## 5.13 Will merchants' PoS equipment need upgrading?

Yes, but The Logic Group's Smart-Switch is designed to interface with any PoS environment, making any changes quick and easy.

Merchants will need a chip card reader and PIN pad in order to read the data from chip cards and allow the cardholder to enter their PIN. Smart-Switch is designed to work with a range of card readers and PIN pads as well as a variety of validation/authorisation applications.

## 5.14 What are the benefits of Chip & PIN?

- There will be less payment card fraud
- Security will be improved
- Transactions will be faster at point of sale because PIN is faster than signature
- Multiple applications can be stored on one card
- Unattended payment devices can be utilized more safely.

## 5.15 What is EMV migration?

EMV migration is the transition from magnetic stripe credit and debit cards to chip cards and is intended to cut payment card fraud.

## 5.16 What is EMVCo?

EMVCo is an organisation formed by Europay, Mastercard and Visa to oversee the implementation of Chip & PIN cards.

EMVCo maintains and develops a set of specifications to ensure global operability, so that any EMV-accredited card can be accepted at any EMV-accredited point of sale anywhere in the world.

## 5.17 Do merchants have to obtain EMV approval?

No. The Logic Group's Smart-Solution is EMV approved at Level 2.

Smart-Solution incorporates The Logic Group's Solve/SE validation/authorisation software and Smart-Switch, for dealing with smart card transactions. Smart-Switch is a Level 2 EMV-approved application that can interface with any PoS environment, a range of PIN pads and card readers and a variety of validation/authorisation applications.

The Logic Group is working with all the major card reader and PIN pad manufacturers so that they can offer solutions with full EMV Level 1 and 2 approval. The Logic Group ensures that all hardware components supplied with their software have been granted EMV Level 1 accreditation.