



Chip and PIN Implementation Guide for Retailers



Produced by The Chip and PIN Programme Management Organisation

The Purpose of this Guide

The purpose of this guide is to give retailers with their own integrated or stand-alone Point of Sale (PoS) equipment an overview of some of the operational and technical considerations they face as they plan for and implement chip and PIN, including best practice guidelines.



Contents

■	1. What is chip and PIN?	5
■	2. What do I need to know?	9
■	3. How do I make this happen?	13
■	4. Doing it!	21





1. What is chip & PIN and why is it happening?

2002 card fraud losses amounted to £425 million. If the chip and PIN system is not put into action, forecasts show that UK losses would be in the region of £800 million by 2005. If this were allowed to happen, the survival of the card payments system could be in jeopardy and this would impact heavily on the retail sector.

In recent years payment card fraud has increased significantly in most countries in the world. The number of cards issued and in use has also grown.

Much of the money obtained from card fraud is used to fund other crime such as drug trafficking, illegal immigration and terrorism. Other crimes like burglaries, muggings and car break-ins are often motivated by the opportunity to steal payment cards.

Card fraud losses will reduce considerably with the introduction of the chip and PIN system, supported by a range of other prevention initiatives including the pilot of a police unit dedicated to combating organised card criminals.

The retail and banking industries, alongside police and with support from the Home Office, will continue to work together to beat the UK's card fraud problem.

To combat card fraud, two things need to be established at the time of the transaction: that the card is the genuine item and that the person using it is the true owner. Chip and PIN is a major development in combating fraud. Instead of using their signature to confirm a transaction, cardholders will use a four-digit PIN, as they currently do when using a cash machine.

Chip and PIN is built upon new international chip specifications known as EMV, that were developed by the major payment schemes (Europay, MasterCard and Visa) – www.emvco.com.



Transition and Maturity

The aim of the chip and PIN programme is to reach maturity through a period of transition.

- **Maturity** is defined as the point at which the only acceptable means of cardholder identification at a chip and PIN PoS with a PIN capable card is PIN. There will not be an opportunity to revert (“fall back”) to using signature or magstripe.
- **Transition** is defined as the period at the beginning of migration during which a chip and PIN cardholder may be allowed, with the retailer’s agreement, not use their PIN at a chip and PIN capable PoS, because they do not know it or have forgotten it – that is they may fall back to using chip with signature.

Liability Shift

The international card schemes (VISA and MasterCard) have each mandated – effective 01 January 2005 – that the liability for fraudulent transactions at the point of sale will shift to the non-chip & PIN enabled party, where fraud could have been prevented by PIN.

If participants have complied with the card schemes’ mandates and cardholders are successfully authenticated, then the issuer must take responsibility if the transaction later proves to be fraudulent.

Note: card not present transactions (e.g. mail order, telephone order and Internet transactions) are **not** covered by this liability shift nor are they affected by chip and PIN. There are separate fraud prevention programmes in place to cover this type of transaction, for which merchants have traditionally not enjoyed a payment guarantee. With these new programmes, there are opportunities for merchants to secure a guaranteed transaction.



Checklist

- Establish the facts
- Talk to your acquirer to establish the effect chip & PIN will have on your business



2. What do I need to know?

The Northampton trial completed successfully at the end of August 2003. There was a significant amount of learning that has been captured during the trial that will be of use to retailers during rollout.

A good starting point for information and detailed learning from the trial is the official UK chip & PIN website, www.chipandpin.co.uk. This comprehensively covers the scope and activities regarding chip & PIN and holds two important reports for retailers:

- **Rolling out chip & PIN – A retailer guide to lessons from the Northampton trial**
- **Checking out chip & PIN – The Northampton trial report**

Additionally, it is worthwhile contacting the trade association for your sector which will be able to give you guidance and share information about what other retailers are doing and what is working well.

As this is a technology-driven initiative, you should speak to as many hardware and software suppliers or vendors as possible. Different trading environments require different solutions and shopping around will better inform any business decisions that you need to make. It is imperative that the solutions you consider are EMV compliant.

Accessibility

Retailers must consider accessibility issues which people may have in your store. The amendments to the Disability Discrimination Act (DDA), coming in 2004, mean that this is a very topical consideration.

The introduction of PIN at PoS will represent a substantial improvement for a significant proportion of disabled customers, both those that are already using cards and those that are not, and particularly those suffering from problems associated with mobility, manual dexterity, use of hands, physical co-ordination and sight. For example:

- the difficulties experienced by some cardholders relating to signing may be avoided;
- the difficulties of handling notes and coins may be avoided;
- the difficulties of using cheques may be avoided; and
- in many outlets, the provision of hand-held terminals that could be taken to disabled customers could facilitate easier transactions.



Nevertheless, it is acknowledged that PIN may not be ideal for everybody, such as individuals with disabilities relating to memory problems, concentration problems or learning difficulties who may be unable to remember a PIN. In these cases it will be possible for an alternative solution to be provided to the cardholder by their card issuer.

Readers are encouraged to obtain a copy of the **Retailer Route Map for Accessibility** from the Chip and PIN Programme Management Organisation, or the chip and PIN website www.chipandpin.co.uk. There is also a section on accessibility considerations for retailers on the chip and PIN website.



Checklist

- Obtain copies of the reports, **Rolling out chip & PIN** and **Checking out chip & PIN**, available at www.chipandpin.co.uk
- Contact the trade association for your sector to gain insight and learning from your peers
- Speak to as many suppliers/vendors as possible to build awareness of different solutions so that you can tailor for your retail environment
- Consider accessibility issues and the potential impact of the DDA





3. How do I make this happen?

The successful introduction of chip & PIN will most likely be a high priority for your organisation. Planning and internal buy-in are vital to ensure timely delivery.

Retailers should set up an internal project team, probably led by store operations. This team will ensure the involvement of all necessary areas across your business and also integrate any 3rd party vendors or consultancy support that you employ. An initial assessment of the overall resource and skill level should be considered during planning. This will allow you to contract additional resource or consultancy in order to ensure on-time delivery.

The plan should be agreed by all stakeholders, internal and external, and should pay particular consideration to the amount of time required for certification, testing and re-testing. This was a major learning point from the trial.

You should evaluate how chip & PIN will operate in your particular retail environment. As outlined in section 2 above, there are a variety of technical solutions available. The degree of process complexity will have a direct impact upon overall project timescales and costs. Again, consideration must be given to accessibility for those customers who have disabilities.

Development of training material and plans is imperative to facilitate the seamless introduction of the new system. It is never too early to start constructing

this material. This is important as it should mean less disruption to customers and queuing and maintain a pleasant customer experience.

From a business perspective, it is vital that you understand the business drivers and success criteria that you operate under. These must be clearly articulated and understood from the outset. Again, the trade association for your sector should be able to provide help in constructing a business case for chip & PIN.

Common Operational Processes

Whilst it would be highly desirable to have a common point of sale operation the diversity of point of sale environments makes a common operation impractical. There is, however, a need to define the general procedure at the point of sale that all retail environments should follow as closely as possible. The need for this common process is twofold; first to try and provide a similar experience for cardholders at all points of sale and second, to simplify training of point of sale staff, particularly if they change trading environments.

In the examples shown below there are suggested displays for both the point of sale cashier and the cardholder. Particularly for the cashier, these examples are only intended to convey the type of action required – the actual wording will reflect the ‘in house style’ of the retailer and their system. Additionally any display for either the cashier or the cardholder will be constrained by the capabilities of the devices available. So where a self-service kiosk would have the ability to provide full graphics or even video to guide the cardholder through the transaction, a minimum specification PIN pad may only have two lines of sixteen characters.

For example a large display could display the PIN entry prompt as:

```
Amount £25.35
Enter PIN
Then press Enter or
press Cancel to clear
```

A two by sixteen display would not have this capability and may manage this as shown below:

```
Amount £25.35
Enter PIN
```

When the first digit of the PIN is entered the display would change:

```
PIN
OK=E CANCEL=C
```

Card Handling

One of the advantages of a Chip and PIN environment is that it allows the customer to keep sight of their card at all times. There will be 2 modes of operation within a retail environment, one where the customer dips their card themselves and one where the customer hands over their card to the cashier to dip. The retailer will have to inform the customer whether to “insert card” or “hand over” card to cashier.

Cardholder Messages

Retailer instructions will be displayed on the terminal. Cardholder instructions will be displayed on the PIN pad.

To ensure consistency in the messages displayed by the terminal and the PIN pad, adherence to EMV defined specifications for standard messages is strongly recommended. EMV specifications can be found on the EMVCo website www.emvco.com.

Cashier messages and procedures

Cashier messages on the till will be different from the customer PIN pad prompts. The cashier messages must be followed closely in order to avoid error and a supervisor called if any messages are not understood or if an error message is shown.

Vouchers and receipts

In the magnetic stripe environment a payment voucher is produced. This may be a two or three-part voucher on some PoS terminals. On other PoS devices and on many PoS systems tandem printing is used – that is a retailer copy is produced first for signing then the cardholder copy is produced.

There is no need with chip and PIN to produce a separate voucher on a PoS system; in particular

there is no need for the retailer copy for the purpose of responding to **Request For Information** (RFI) to defend chargebacks. RFIs will disappear for successful chip and PIN transactions in a mature environment. Retailers will be able to produce evidence from stored electronic data if needed.

Cardholders will still need the option to have something for their records but this need not be a separate voucher. The card payment data can be included at the bottom of the PoS itemised receipt. The information to be displayed should include an indication **PIN Verified**.

Some retailers may retain vouchers for their own internal procedural needs: to balance the till or for audit where Purchase with cashback (PWCB) is offered.

Purchase with Cashback

In a magnetic stripe environment the Issuer Identification Number (IIN) is used by the application in the PoS to determine if the cardholder is able to have cashback on the card product. Purchase with cashback (PWCB) on a chip card is determined by data in the chip.

Additionally even if the card allows PWCB it is a retailer option whether to offer the service and if they do, some retailers wait for the cardholder to request cashback whereas others ask the cardholder if they want cashback. Both forms of operation are permitted. Maximum cashback limits (subject to scheme rules) are negotiated between retailer and acquirer and are therefore a PoS parameter.

Where cashback is taken it is preferable for the cash element to be displayed separately to the cardholder before PIN entry. However the total (purchase + cashback) **must** be displayed prior to PIN entry.

Regardless of whether the cash element is displayed it must be shown on any cardholder 'voucher'.

Premature Card Removal

The card should not be removed from the terminal until prompted by the terminal.

Refunds

Refund transactions are outside the scope of EMV and card schemes do not require that terminal or card risk management be performed. If the full EMV process is used, PIN will be required and the card may request online authorisation and authentication.

It should be noted that Acquirer and Issuer systems must be able to process refund transactions both with and without chip data.

Retailers therefore have two options:

a) Read either the Track 2 equivalent data or its component parts from the chip; do no further processing with the card;

Or

b) Perform a full EMV transaction, including CVM list processing and PIN checking if applicable.

Declines

Within the EMV process a transaction can reach a declined result through three paths:

1. The card can decline the transaction based on internal risk and usage parameter checks
2. The terminal can decide that the transaction should be declined as a result of risk and usage parameter checks
3. The card issuer can request that the transaction be declined as a result of on-line authorisation and authentication.

In addition to declining the transaction the issuer can (as with any response) send a script to be acted on by the card and / or may also request that the retailer retains the card.

Where the transaction is declined the cashier will be aware on their display that the transaction has been declined. For display to the cardholder the term **Not Authorised** is preferred.

The point of sale should provide the cashier with as much additional information as to the reason for the decline to aid communication with the cardholder. Examples would be:

1. Transaction declined after on-line authorisation – additional cashier display **Issuer Decline – Cardholder Should Contact Issuer**
2. Transaction declined by the card – **Declined By Card – Cardholder Should Contact Issuer**

If the transaction is declined then the data collected is discarded and the cardholder's card is returned along with any completed transaction voucher/receipt showing that it has been declined. Where the transaction is declined no settlement data will be presented but the retailer's system should keep a full audit trail.

The wording used on any PoS system should be chosen to fit in with the retailer's mode of operation and training at the point of sale. The retailer may also be limited to the number of characters to be used. Its aim is to inform the cardholder and support the cashier in what can be an awkward situation.

A transaction declined by the card, terminal or card issuer may not be reprocessed using alternative data entry (magstripe or manual entry of card number (PKE)).

Decline and Retain

In exceptional circumstances the retailer may be requested (through the APACS30/40 response code as today) to retain the card (also known as **decline and pickup**). This will normally be sent in conjunction with a **block application** or **block card** script, which prevents the card from carrying out further chip transactions. The **retain** message should not be displayed to the cashier until the card has processed the script.

If the card is in the cashier's hands, or in the card reader, retention should not pose a problem. However, if the cardholder has inserted the card the cashier should either remove the card or ask the cardholder to remove it when indicated and then ask for the card. Cashiers should not attempt to grab the card or put themselves at risk in order to retain the card.

Referral

In response to an on-line authorisation request the Issuer may return a referral response that requests the merchant to make contact before the transaction can be completed. In the mature chip and PIN environment it is anticipated that the reason for most referrals will be security checks where the cardholder's spending has been flagged as unusual behaviour.

In order to leave the chip in a known good state the EMV part of the transaction is completed with the card as though it had been authorised. The retailer's normal procedures will then be followed. In a smaller retailer the telephone call to the Acquirer's Authorisation service centre will probably take place from the point of sale. In larger retailers or multi-lane environments the transaction may be 'laid away' on

the Point of Sale and the cardholder taken to a customer service point where the transaction will be recalled and completed.

It may be possible to provide all of the information requested during the Referral Call from data printed on the voucher/receipt. It is recommended that the card is removed when prompted as information may be required that is not on the receipt (for example the Card Security Code on the signature strip).

If the transaction is authorised the authorisation code is added to the data collected up to the point of referral; these are used to complete the transaction and for settlement. The cardholder's card is returned along with the completed transaction voucher / receipt.

If the transaction is declined:

- the completed transaction should be reversed or cancelled within the PoS system;
- no further processing is done with the card (i.e. the card believes it has completed the transaction);
- no settlement data is sent in respect of the transaction.

Reversals

Reversals are used to undo transactions that have been performed in error. This is usually where the transaction has been sent on-line for authorisation and then the cashier or the cardholder notices that the amount of the transaction is incorrect. In the magnetic stripe world this will often happen when the cardholder signs the voucher. By this time the PoS has already begun, if not completed, the on-line authorisation.

In a chip and PIN environment the PIN is input early in the EMV transaction, before the card and PoS have determined if this transaction needs to be sent on-line to the Issuer. The amount is displayed to the cardholder before PIN entry. This means that the number of transactions that need to send a reversal message should be reduced.

There will, however, be transactions where an error is noticed or the cardholder decides at the last minute that they do not want all of the items for this transaction and authorisation is already taking place. In a standalone terminal the whole transaction will have to be undone but in a PoS system it is just the tender element that needs correction and it may be possible to keep the purchase transaction 'alive'.

It is important that the chip on the card is left in a known stable state and the action taken will depend on the point reached in the EMV process.

If an authorisation request has been sent to the acquirer the response must be processed as it may contain a script from the Issuer. Having processed the response message, the PoS should use the EMV process to close down the card transaction.

In all cases the PoS should produce a receipt/ voucher for the cardholder (which may be on the till receipt) showing that the original payment has been voided. For standalone devices the payment transaction will have to be restarted. For PoS systems the transaction may still be 'alive' and a new tender process can be started within the transaction.

Handling PIN problems

There may be situations where the cardholder is unable to use PIN when required by the terminal due to not knowing the PIN value or having exceeded the allotted number of PIN tries.

Pin bypass

The Cardholder Verification Method (CVM) list in cards defines which CVMs the card supports, in what order they are to be applied and what must be done if the CVM is not supported or fails. Cards issued in the UK will have PIN as the primary CVM at the point of sale if a PIN pad is available. If PIN is not supported then the card will be able to use the next CVM, which will normally be signature. If PIN verification fails, then cards issued in transition will normally also allow fallback to signature. Once issuers start to issue cards in maturity, they are likely to issue chip cards that will not permit fallback to signature in the event of PIN failure; the action will be to decline the transaction.

This means that if a cardholder inputs their PIN enough times incorrectly (three times for most UK issued cards), so that the PIN is locked, then the PoS will automatically move to the next CVM, which is assumed to be signature. In the transition period a means is needed to allow cashiers to bypass PIN entry because the cardholder has forgotten their PIN without having to lock it. It is recommended that a key on the cashier keypad be allocated to **PIN bypass**, and that this key may be enabled or disabled using a single parameter which can be configured by the retailer. Where PIN bypass is used, the terminal must always seek issuer authorization.

Some retailers may elect to keep this functionality for exceptional situations or to serve disabled customers better. For example it is probable that a cardholder confined to a wheelchair will be able to use the PIN pad in most face-to-face 'in-store' transactions. This probably will not be the case at petrol stations, where the cardholder will still require a member of staff to collect their payment card, produce a 'fallback' signature receipt and return this to the cardholder to sign.

Whilst such cardholders' cards could be configured not to support PIN at PoS to overcome this need, this could be seen as disadvantaging the cardholders by excluding them from using PIN in other environments. Issuers must improve their knowledge of their customers to identify these types of cardholder and the problems they face.

What is the effect if the PIN is locked?

The PIN is locked if the wrong PIN is entered 'n' times in succession at the point of sale although not necessarily in the same transaction. Although this is normally three consecutive attempts, retail systems must not assume this figure.

Once the number of PIN tries has been exhausted, the application will not carry out any further offline point of sale transactions; however the card may still be used if the CVM list allows it. This may then enable an online signature-based transaction.

Locking the PIN at a point of sale will not prevent the cardholder from using an ATM if they subsequently remember their PIN, or from using a chip terminal that does not support PIN. This may be confusing for customers and it is strongly recommended that customers always call their card issuer for assistance.

How can the PIN be unlocked?

If the customer locks his or her PIN at a point of sale in the UK, it can only be unlocked at an ATM.

The issuer will advise the cardholder how they can unlock their PIN. Normally, this will be by going to an ATM and selecting “PIN Services – Unlock” (or PIN Change). The cardholder will need to know their PIN to perform this operation.

What messages should be given:

Cardholder

In every case where a PIN is locked, in the current or previous transaction, the cardholder should be given the message **PIN Locked – Call/contact card issuer**. The cardholder will then be given full instructions by the card issuer.

This applies whether or not the retailer was able to (and agreed to) continue with the transaction.

Retailers, at their option, may print **PIN Locked – call/contact card issuer** on the POS or EFT receipt.

Cashier

The cashier cannot tell from visual inspection whether or not a chip card is PIN-enabled. The card will either ask for a PIN or a signature, as appropriate.

Following a request for a PIN, if a PIN is locked on the current transaction, the transaction will normally be declined and cannot be restarted using the same card. The cashier should be given a similar message to that currently given for declined transactions. Cashiers should wherever possible reinforce the **call/contact card issuer** message.

During the transition period, issuers may permit a signature-based transaction with online authorisation if the PIN entry fails. In this case, the cashier should be advised to proceed with the transaction but to take particular care over checking the signature. This could be achieved by displaying a message **PIN locked – check signature**.

If the PIN has already been locked, the card may still be usable for a signature-based transaction with online authorisation. Cashiers should still draw customer’s attention to the fact that the PIN is locked, and should again exercise particular care over the signature check in this case.



Checklist

- Set up an internal project team, probably led by store operations
- Agree a timebound project plan with all stakeholders especially 3rd party suppliers and vendors
- Build in sufficient time for certification, testing and re-testing
- Consider the Common Operational Processes recommended by the Programme when documenting your requirements and training plans
- Start to build training plans and awareness from the outset
- Clearly understand your business drivers



4. Doing it!

After documenting your specific requirements, go out to tender following your company's procurement process. You should ensure that hardware and software products offered are certified by EMVCo or that you are comfortable with supplier plans to achieve this certification.

Set up an internal pilot to test the functionality of both the technical and operational processes of chip & PIN. This will be valuable in 'ironing out' any bugs or glitches that you might find, finalising the training material and most importantly establishing any pre-requisites for acquirer acceptance testing.

As outlined previously, the approvals process can be quite lengthy and time should be built into the plan to reflect this. There are four phases of the certification process of which retailers need normally concern themselves only with the last two.

Phase 1

- EMV Level 1 certification of the card reader hardware/firmware
- Visa Security Certification (offline PED)
- APACS PED Security Evaluation

Phase 2

- EMV Level 2 certification of the kernel software

Phase 3

- Visa end-to-end certification
- MasterCard Terminal Integration Testing
- AmEx and JCB offline testing

Phase 4

- Acquirer connectivity tests

You should contact your acquirer for further details of phase 3 and 4.

After your solution has been successfully approved, implementation will follow. There are a number of other considerations for rollout that should minimise any disruption to your operations and the customers' experience.

Security at POS

It is important that the customer's PIN is not compromised at the point of sale. The PIN pads should be positioned in such a way that neither the cashier nor other customers can see the entering of the PIN by a customer. CCTV cameras must also be positioned in a way that they do not overlook the PIN pad.

Retailers should also ensure that adequate systems are in place to ensure that the entering of the PIN cannot be seen over someone's shoulder (shoulder surfing).

Fallback

A fallback situation occurs where the transaction cannot be performed with the primary technology. This may be the inability of the terminal to read the chip or where PIN entry cannot be performed when required.

Chip Failure

Technology fallback for a chip card transaction is caused by a failure (before or during the transaction) of the chip on the card, of the chip reader or of the terminal supporting the chip card transaction.

In some cases, failure of the PIN pad would result in the terminal being unable to process chip transactions. It is preferable that the terminal should be able to carry out chip transactions if the PIN pad fails, but this may often be impractical or uneconomic.

What should the retailer or its terminal do?

Initially, terminals and procedures should be set up so that if a chip card or reader fails:

- a) the transaction may be completed using the magstripe and signature, but with online authorisation (zero floor limit). (The magnetic stripe data will identify to the issuer that this was a chip card and it can take appropriate action). The “reason online” code must indicate that this is a fallback transaction;
- b) if the magstripe cannot be read, the card should be declined (i.e. there should be no fallback to manual entry of card number (PKE) on a chip card). This will often require a manual procedure or decision.

If either card or reader is magstripe-only, and the magstripe cannot be read, the transaction may (if permitted by the terminal) be completed using PKE.

Signature Fallback

Signature fallback applies where a Chip and PIN card meets a chip and PIN terminal, but:

- the PIN pad itself is faulty (but the reader is still able to read the chip)
- OR the cardholder is unable or unwilling to enter their PIN correctly
- OR the PIN has been locked

What should the retailer or its terminal do?

If the PIN pad is faulty, but the chip reader is still able to read the chip on the card, then, dependent on the configuration of the card and terminal, the transaction may be completed using chip and signature with online authorisation.

If the cardholder is unable or unwilling to enter his or her PIN, the retailer has the option (if permitted by the card and terminal) of allowing a signature-based transaction with online authorisation. There are several possible scenarios:

- a) Cardholder states at start of transaction that he/she cannot remember PIN;
- b) Cardholder enters PIN wrongly once or twice, but then asks to use signature before locking PIN;
- c) Cardholder locks PIN by entering PIN wrongly ‘n’ consecutive times;
- d) PIN already locked at the start of the transaction.

These scenarios have been covered in the section **Handling PIN problems**.

In the first two cases, there is a need for a PIN Bypass facility as discussed above, if the terminal/retailer allows this fallback mode.



Checklist

- Ensure that hardware or software products are EMVCo certified
- Set up an internal pilot of the new system to test technical & operational issues
- Conduct acquirer acceptance testing and ensure your system is type approved
- Ensure implementation and training plans are in place
- Consider PIN security measures and Pinpad placement
- Go for it!

Further Information

The Chip and PIN Programme Management Organisation has published a number of other documents, including two reports on the Northampton chip and PIN trial which you may also find useful in planning your chip and PIN implementation. These documents are available to download from the chip and PIN website www.chipandpin.co.uk/library/index.html

www.chipandpin.co.uk

Further Information

For further information, please contact the Chip and PIN Programme at info@chipandpin.co.uk

Chip and PIN Programme, PO Box 44737, London SW1P 1RF

Telephone: 020 7960 6012 Fax: 020 7960 6100 www.chipandpin.co.uk