EPC343-08
Version 2.0
8 December 2016

European Payments Council

[X] Public – [ ] Internal Use – [ ] Confidential – [ ] Strictest Confidence

Distribution: Publicly available

PRIVACY SHIELDING FOR PIN ENTRY

Conseil Européen des Paiements AISBL– Cours Saint-Michel 30A, B-1040 Brussels
Tel: +32 2 733 35 33 Fax: +32 2 736 49 88
Enterprise N° 0873.268.927 www.epc-cep.eu secretariat@epc-cep.eu

Document History

This document was first produced by EPC as DIG114 v1.0 in 2006. EPC has revised the document in view of the new developments on this topic and published a new version with an EPC cover page and new number (EPC 343-08 v1.4) in 2009.

The present document is a new update of EPC 343-08v1.4; the introduced changes aim to improve the clarity, to update references and to make some corrections in figures 1 and 3.

Devices that could be claimed to have met the previous requirements should still be compliant to this new version of the document.

TABLE OF CONTENTS

1 Introduction

Privacy shielding is one of several means for reducing the risk that cardholder PINs are observed during PIN entry. In addition to the provision of a shield:

- cardholders need to be educated to use their body and hands as shields when entering their PIN
- merchants need education on the proper deployment of PIN entry devices, especially with respect to customer queues and in-store security cameras
- cashiers need education on the proper use of PIN entry devices.

Acquirers and domestic payment organisations in different countries have defined their own requirements on privacy shielding. Consequently terminal manufacturers need to comply with different requirements and cardholders may be faced with differing configurations within a country and across Europe.

This document identifies common criteria for privacy shielding for POS and ATMs in a variety of environments. It is based on existing European hardware requirements and the work executed by PCI (Payment Cards Industry) for POS, aiming to provide refinements and additions as appropriate.

It is recognised that existing requirements and installations are not always compliant and that it may take years to align them, even if taken up throughout Europe. However, this document aims to support the SEPA Cards Standardisation Volume (EPC 020-08) objectives of a consistent customer experience with regard to the use of cards and terminals and to further reduce the risk of fraud resulting from shoulder surfing. It also contributes to a further harmonisation and standardisation and may be used by payment service providers and payment organisations in discussions with terminal suppliers.

2 References and Definitions

2.1 References

The following documents and papers have been reviewed in preparation of this document:

Ref.	Title
[1]	CEN TS 15291: *Identification card system – Guidance on design for accessible card-activated devices,* 2006.
[2]	Chip and PIN Programme, UK, *Programme Guideline G16 – Privacy Shields*, version 1.1 (17 February 2004) (see also www.chipandpin.co.uk).
[3]	ISO 9564: *Banking -- Personal Identification Number (PIN) management and security – Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems, Annex G (informative) Information for customers,* 2011.
[4]	Payment Card Industry (PCI), *POS PIN Entry Device, Derived Test Requirements, Appendix A – Criteria for the Privacy Screen Design,* Version 2.0, April 2007.
[5]	Payment Card Industry (PCI), *PIN Transaction Security (PTS) Point of Interaction (POI), Modular Security Requirements*, version 4.0, June 2013.
[6]	Pan-Nordic Card Association *Exterior Shield - Ver F Final - Best Practice*, 18 March 2013.
[7]	PBS, Denmark, *Open Terminal Requirement Specification, Attachment H: Privacy Shield on PIN Entry Devices*, Version 2.2.1, 2 April 2003.
[8]	ZKA, Germany, *Requirements for the assessment of privacy shields in PIN pads*, Version 1.0, April 2004.

Table 1: References

2.2 Definitions and Abbreviations

Term	Definition
ATM (Automated Teller Machine)	An unattended mechanical device that permits authorised users, typically using financial transaction cards, to access financial services including cash withdrawal.
Acquirer	A Payment Service Provider (i.e. financial institution, its agent, ...) which acquires from the merchant the data relating to the transaction, and initiates that data into an interchange system.
Attended terminal	A card-accepting terminal requiring the involvement of a terminal operator / cashier.
Cardholder	A customer associated with the account identification on the card or customer owning the card in the case of anonymous card products not related to any account.
Desktop terminal	A payment terminal operated on the desk of the merchant during the payment transaction when a PIN may be entered; it may be either a terminal permanently installed on the desk or a portable terminal with such characteristics that the cardholder will not use it in his hands.

Handheld terminal	A payment terminal operated by the cardholder, during the PIN entry phase of the payment transaction, in the hand of the cardholder, which may then protect the PIN entry from any shoulder surfing.
Observer	A person or device that attempts to discover the PIN by observation.
Payment Card Industry (PCI)	A consortium of the following card schemes, Visa, MasterCard, American Express, JCB and Discover, which became formalised as the PCI Security Standards Council or PCI-SSC and which manages various aspects related to common industry security requirements.
PIN entry device (PED)	Device into which the cardholder inputs the PIN. A PIN entry device may also be called a PIN pad.
PIN entry device (PED) keypad	A keypad with an arrangement of numeric, command and, where required, function and/or alphanumeric keys laid out in a specific manner.
PIN shielding	See privacy shield.
Portable terminal	A payment terminal which may be moved up to the cardholder environment, for instance in a restaurant. A portable terminal may be considered as a handheld device if it fulfils the physical requirements and is used alike by the cardholder.
Point of Interaction (POI)	An electronic-transaction-acceptance product. A POI consists of hardware and software and is hosted in an acceptance equipment to enable a cardholder to perform a card transaction. Thereby the POI may be attended or unattended. POI transactions are IC and/or magnetic-stripe card-based payment transactions.
POS	Point of sale (as used in ISO 9564-1, [3]) or point of service (as used in EMV 4.3 and in ISO 8583).
Privacy shield	A physical barrier around the PIN entry device deterring the visual observation of the PIN values as they are being entered by the cardholder.
Shoulder surfing	A way of using direct observation to gather confidential information, usually password or PIN that can be used to gain access to a secured system. The term has its origin in the practice of physically looking over someone's shoulder while they are typing in their password.
Unattended terminal	A cardholder operated device that reads, captures and transmits card information in an unattended environment, including, but not limited to, ATMs, automated fuel dispensers and load devices. So there is no cashier that accompanies the terminal and the payment.

Table 2: Terminology

3 Scope and Background

3.1 Scope

PIN entry must be performed in such a way that the PIN entered by the cardholder cannot be easily observed. This includes direct observation by cashiers, checkout attendants, other customers and people nearby, remote observation using binoculars or other aids, plus technological devices such as cameras. Note that cameras may include legitimately placed devices such as store and ATM security CCTVs as well as spy devices such as pin-hole cameras or web-cameras. Therefore, it is recommended that the PIN entry device be equipped with shielding to deter the visual observation of the PIN values as they are being entered by the cardholder.

In addition to the physical PIN pad design, attention must be given to the proper installation of the PIN entry device, the education and or training of the cardholder, merchant and any party involved, and PIN protection policy enforcement. The design also needs to consider the requirements of disabled persons.

This EPC document is based on an analysis of the Payments Cards Industry (PCI) hardware requirements covering MasterCard and Visa and a number of representative European national requirements. Given certain differences between the PCI requirements on the one hand and the national ones on the other, this document:

- defines criteria for the privacy shielding – what to protect, how to install the privacy shield and the specific angles of protection that are common to all devices and environments
- defines privacy shielding criteria for specific devices and environments from portable handheld devices to ATMs.

Given the large number of issues and concerns associated with privacy shielding, the Annex collates these issues, including the importance of the awareness of the cardholder of PIN capture through shoulder surfing and how they can protect against this risk.

3.2 Background: PCI and National Requirements

This document describes measures aimed at protection against illicit PIN entry observation by shoulder surfing and other techniques.

Given the importance of the card scheme participation in PCI, this document is based on a comparison of the PCI requirements and several representative European requirements (see section 2 for references).

The main differences are:

- While both use the concept of a circular segment of 270 degrees with an opening facing the cardholder, the PCI protection angles vary from 35 to 40 degrees while the national requirements vary from 35 to 45 degrees.
- PCI specifically distinguishes handheld devices as those that do not require a privacy shield for this confirmation, since the cardholder should serve as the shield. Many national specifications do not distinguish between handheld and non-handheld devices.
- PCI introduces the concept of vertical installations, a concept that is rarely or not addressed in national requirements.

4 Privacy Shielding Requirements

4.1 General Privacy Shielding

- The shield design is to deter the visual observation of the PIN values as they are being entered by the cardholder during PIN entry; the shield need not be designed to deter the visual observation of the command keys (see Annex B) such as CANCEL, CLEAR and ENTER, nor the display screen.
- The shield and the cardholder's body in combination are intended to protect against shoulder surfing from many angles, based on PIN pad being at a typical counter top height and for observers standing at the same level as the cardholder.
- The shield design needs to allow full visibility of the keypad by the cardholder, notwithstanding that the cardholder may cover the keys with his or her hand. For example, shields resembling hoods have prevented cardholders from seeing the keypad.
- The shield design needs to allow the display screen to remain visible during PIN entry.
- The shield design is not to limit the operations of the card reader, the command keys or other operations of the terminal or device.
- Preferably, the shield is an integral part of the total design of the terminal/device. The privacy shield shall be constructed in a tamper evident way.
- The shield design needs to allow for use by both right-handed and left-handed cardholders, with a variety of typical hand sizes.
- The shield shall be built in non-transparent material and shall be non-reflective.

4.2 Physical Privacy Shielding Requirements

4.2.1 Basic Concepts

The aim of this section is to define the physical criteria for privacy shielding. However, before describing these requirements, a number of basic concepts are defined to provide the basis for calculating the height and position of the shield.

The **Reference Point** is the central point of a circular Protection Zone and is defined as the centre of the numeric key '5'. The Reference point is the same irrespective of the size of the command keys, or whether they are laid out in a column to the right of the numeric keys, or in a row below the numeric keys. Similarly, if the function keys are absent (e.g. soft keys) or separated from the numeric keys (e.g. larger keys to one side), the reference point is the centre of the numeric key '5'. See Figure 1 below.

The **Protection Zone** is the zone to be protected. It is the area defined by a horizontal circular segment of at least 270 degrees with the opening facing the cardholder.

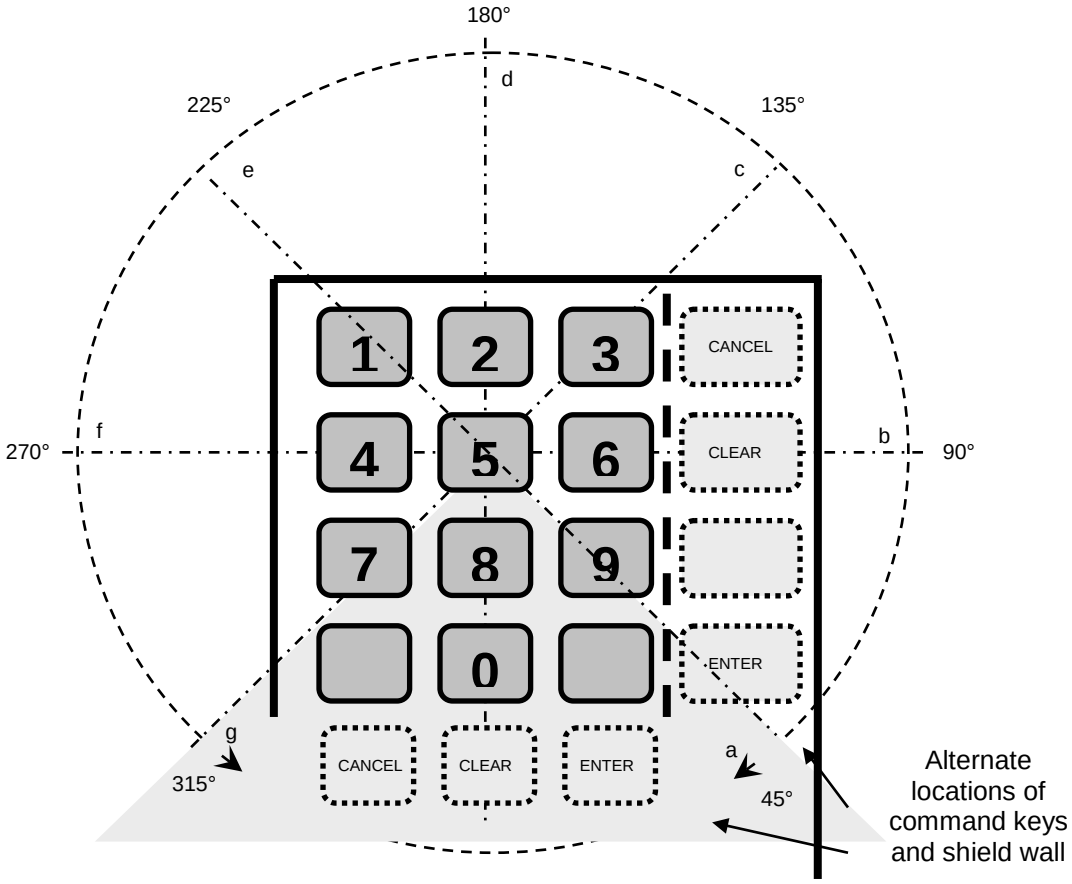

Figure 1: The Reference Point and Protection Zone

Figure 1 illustrates the Reference Point for both the vertical and horizontal layout (see Annex B) and the Protection Zone defined by a circular segment of 270 degrees.

In order to define physical requirements for privacy shielding, the Protection Zone is divided in six segments of 45 degrees by seven boundary lines, denoted as ‘a’ to ‘g’.

The **Observer’s Line** is the line between the observer’s eye and the Reference Point in the Protection Zone.

Protection Angle is the angle between the Observer’s Line and a plane of reference. It is denoted as ‘α’ in Figure 2. The Protection Angle is used to define the height of the privacy shield. The plane of reference is the Horizontal Plane unless otherwise defined.

Inclination is the angle between the plane of the keypad and the horizontal plane. It is denoted as δ in Figure 2 and is relevant for PIN pads mounted at an angle or for PIN pads with a sloping keypad.

Based on these concepts, the privacy shielding requirements are defined for the horizontal installation and then separately for the vertical installation. Figure 2 illustrates the how the basic concepts relate to one another and depicts the horizontal case.

Note: For PIN pads with function keys to the right of the numeric keys, then in principle the shield on the right hand side needs to be higher and longer if located outside the function keys (solid line) than if located just to the right of the numeric keys (dotted line). However, these are minimum requirements and practical designs will likely have both sides of equal height and length for a symmetrical appearance.

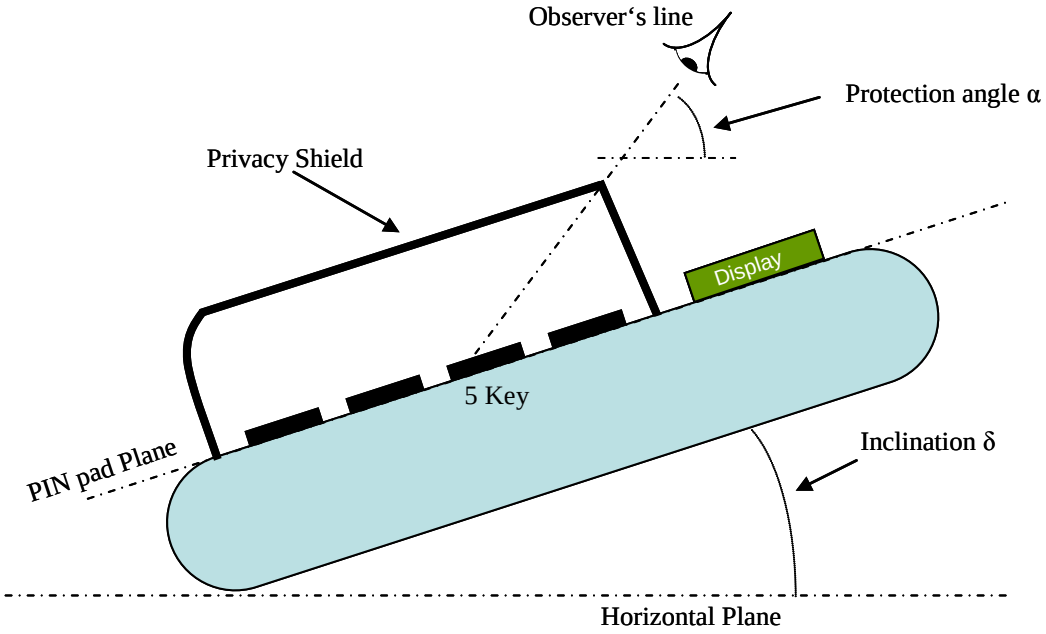

Figure 2: Illustration of the basic concepts (for horizontal installations)

4.2.2 **Horizontal Installation**

Horizontal installations are those where the inclination δ is 45 degrees or less.

The **height** of the privacy shield is determined by a ray from the Reference Point at an angle defined below for six segments of the Protection Zone:

- Between the lines ‘a’ and ‘b’, the protection angle α shall be greater than or equal to 35 degrees
- Between the lines ‘b’ and ‘c’, the protection angle α shall be greater than or equal to 40 degrees
- Between lines ‘c’ and ‘d’, the protection angle α shall be greater than or equal to 40 degrees
- Between lines ‘d’ and ‘e’, the protection angle α shall be greater than or equal to 40 degrees
- Between lines ‘e’ and ‘f’ the protection angle α shall be greater than or equal to 40 degrees
- Between lines ‘f’ and ‘g’, the protection angle α shall be greater than or equal to 35 degrees.

For designs where the keypad plane is not parallel to the horizontal plane, then the inclination δ contributes to the protection angle at the back of the keypad. Thus the height of the privacy shield needed to obtain 40 degrees of protection between the lines ‘c’ and ‘e’ may be less than that required when the keypad plane is horizontal. Furthermore, the height of the privacy shield between lines 'a' and 'b' and 'f' and 'g' would normally need to be increased to maintain the 35 degree protection angle. However, for low values of δ ($\leq$ 20 degrees) then the practical difference is small and using the keypad plane as the reference plane may be considered.

4.2.3 Vertical Installation

Vertical installations are those where the inclination δ is greater than 45 degrees.

The reference plane is the vertical plane. Observation is only possible from the front as the keypad is protected from other points of view by the nature of the PIN pad installation. The **height**[1] of the privacy shield is determined by a ray from the PeferencePoint at an angle defined as follows.

- From the sides, the protection angle shall be greater than or equal to 40 degrees for the whole length of the numeric part of the keypad.

The **length** of the privacy shield is defined:

- on the right side by at least the distance between the lines 'a' to 'c', and
- on the left side by at least the distance between the lines 'e' to 'g'.

Figure 3 shows the length of the vertical installation.

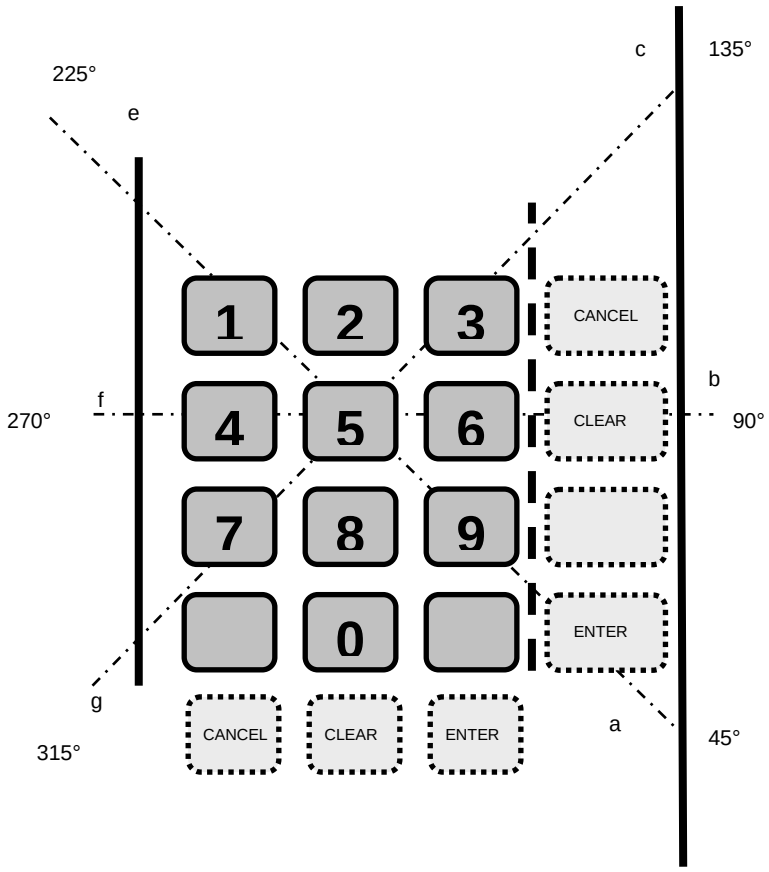

Figure 3: Length of the shield for a vertical installation

Note: For PIN pads with function keys to the right of the numeric keys, then in principle the shield on the right hand side needs to be higher and longer if located outside the function keys (solid line) than if located just to the right of the numeric keys (dotted line). However, these are minimum requirements and practical designs will likely have both the left and right hand shields of equal height and length for a symmetrical appearance.

The shielding requirements for vertical installations are primarily intended to protect

[1] The same terminology is used as for horizontal installations, although shields for vertical installations extend forwards, rather than upwards

against observers standing on the same ground as the user and are necessary on the basis that the keypad is mounted flush on the surface of the terminal. If the keypad can be overlooked from above, then continuing the shield around the top of the keypad is preferable. For some installations the keypad is embedded within the housing of the terminal, in which case the structure of the terminal normally acts as a full and effective shield.

Figure 4 illustrates privacy shielding in vertical installations

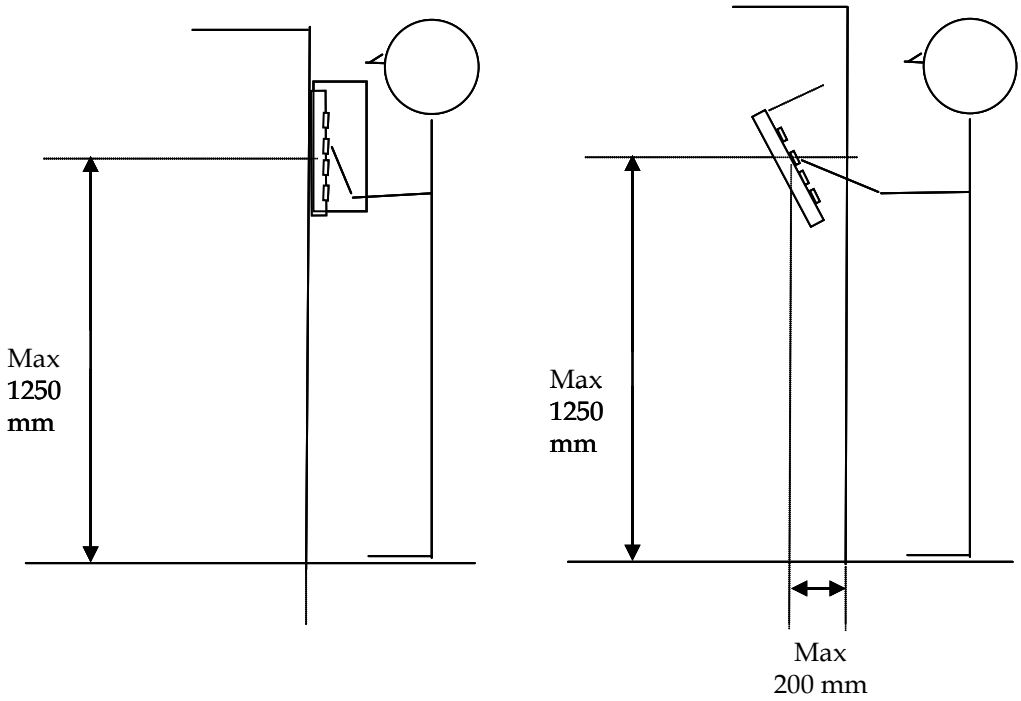

Figure 4: Examples of privacy shielding on vertical installations - keypad on the surface and keypad embedded in the housing of the terminal

4.3 Shielding Requirements for Specific Devices and Environments

The following are requirements for specific devices and environments:

4.3.1 Handheld Devices

Handheld devices, cabled or wireless, should be shielded as a horizontally installed device. While, ideally, a handheld device would not need physical privacy shield, in practice, it cannot be guaranteed that the device would be used as such and hence shall be shielded as a horizontally installed device.

If the payment terminal is fixed to the counter than this payment terminal no longer complies to the definition of a handheld terminal.

For example, a privacy shield is particularly needed where the device is used on a swivel arm or other mounting indicating it will not be used in the hands of the cardholder.

4.3.2 ATMs

ATMs have the PIN pad built into a larger entity which often provides the necessary shielding along with the cardholder's body and hands. Nevertheless these privacy shielding recommendations fully apply to the ATM environment. If necessary, additional

privacy shielding should be added around the PIN keypad

Annex A: Additional Issues relating to Privacy Shielding

i. General Considerations

How the PIN pad is placed in relation to the surrounding environment may affect the risk of PIN capture. Also the placement of the PIN pad in relation to the position of the cardholder may affect the ability of the cardholder to cover the PIN entry device with their body and hands.

ii. Placement of the PIN Pad

When the terminal is set up in the environment where it is to be used, the position of the terminal and the PIN pad need to be convenient for the cardholder, including the possibility to get close to the terminal.

For installations where it is expected that the cardholder will be standing:

- The centre of the keypad surface on the '5' key should not be placed less than 800 millimetres or more than 1250 millimetres above ground level (see the table below).
- It is recommended that the relationship between the height of the keypad above ground level and the angle to the horizontal plane is as follows:

Height (millimetres)	angle (degrees)
800-900	0-30
900-1100	30-60
1100-1250	60-90

Table 3: Keypad metrics

Some devices, e.g. petrol pumps in some countries have special safety requirements on the height of electrical equipment including the PIN entry device, from the ground and this needs to be taken into account in specifying the height of the PIN pad relative to the cardholder for privacy shielding purposes.

When the terminal is installed, the distance from the centre of the surface of the '5' key to the front of the terminal should not exceed 200 millimetres.

(Note: The front of the terminal device is defined as the vertical face of the terminal device (or the base on which the terminal is placed) which restricts the cardholders possibility of getting sufficiently close to the terminal PIN pad.)

Terminal devices should be placed in such a manner as to minimise observation with respect to mirrors, video cameras, staircases, or other similar conditions in the environment.

iii. Positioning of the PIN Pads for POS Terminals

The PIN pad should ideally be positioned behind a fixed partition (such as the cash register) which shields it from the cashier's view. PIN pads should generally be positioned on the side of the customer away from the queue, although care should be taken to ensure that it can be used easily by both right- and left-handed customers. If the queue is directly behind the customer, then the PIN pad should be placed directly in front of the cardholder.

In many situations, it is desirable that the PIN pad can be picked up and passed to someone unable to reach or use the PIN pad comfortably, such as a wheelchair user or

other disabled person or simply a very tall or short person. In these cases, requirements for handheld and portable devices apply.

Installing the PIN entry device on an adjustable stand allows cardholders to swivel the device sideways and or tilt it forward or backwards to a position that makes shoulder surfing more difficult.

iv. Cashier and Cardholder Awareness

Issuing and acquiring banks should advise their cardholders and merchants of the importance of minimizing the risks of shoulder surfing. Merchants should be made aware of how to properly install the PIN entry device to provide a confident environment for the cardholder.

Cardholder awareness is stressed in Annex C “Information for customers” of ISO 9564.

Issuer communications with cardholders should include warnings against shoulder surfing while entering their PINs, particularly in using their body and hands as a shield.

All retailers, for example, could include in their cashier training the topic of privacy shielding, stressing the dangers of shoulder surfing and the use of illicit cameras.

A warning sign or alert sticker encouraging cardholders to protect the entry of their PIN code should be displayed when PIN entry is awaited or the message should appear on a permanent label near the PIN entry device. The following example or similar alert sticker is recommended.

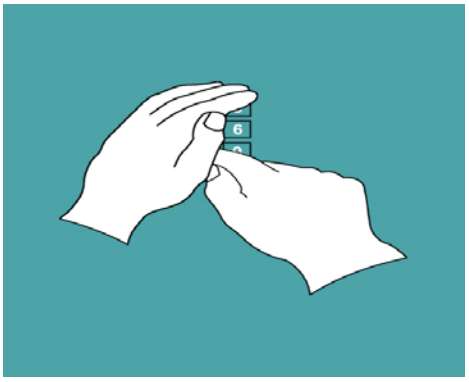

Figure 5: Alert sticker to encourage cardholders to protect their PIN entry

Annex B: Keypad Layout

The following information has been retrieved as reference material from EBS100 Version 3 *Keyboard Layout for ATM and POS PIN Entry Devices,* October 2004.

i. COMMAND AND FUNCTION KEYS - Mandatory and Optional Status

The command and function keys are non-alphanumeric keys and consist of the following:

Command / Function Key	Status
CANCEL	Mandatory
CLEAR	Mandatory on ATM PEDs Mandatory on POS PEDs when command keys are vertically arranged Optional on POS PEDs when command keys are horizontally arranged
ENTER	Mandatory
Additional proprietary key in the vertical layout	Optional
PLUS	Optional function key which is application-dependent It may optionally be used for other functions such as the insertion of special symbols, such as the insertion of '00' or '#'
MINUS	Optional function key which is application-dependent It may optionally be used for other functions such as the insertion of special symbols such as the insertion of ',' or '*'

Table 4: Overview command and function keys

Other optional function keys may be available on a PIN entry device keypad, but are not described, for example, function keys, marked with arrows below or at the side of the screen that are used to activate a function described on the screen.

The use of terms such as CANCEL, CLEAR and ENTER does not exclude other equivalents or their translation in other languages.

ii. Position of the COMMAND AND FUNCTION KEYS

Command keys shall be arranged vertically in a column to the right of the numeric keys, or horizontally in the last row on PIN entry devices.

Vertical layout

The vertical arrangement of the command and function keys shall apply to ATM PIN entry devices and those POS PIN entry devices, where there is sufficient space.

The following specifications shall apply when the command and function keys are arranged vertically:

- The CANCEL key shall be the uppermost key, to the right of the numeric key ‘3’
- The CLEAR key shall be to the right of the numeric key ‘6’
- The ENTER key shall always be the last key in the rightmost column. The Enter key shall be either in the:
    - Third position, if the additional proprietary key is blank, or
    - fourth position, if the additional proprietary key is present
- The optional additional proprietary key in the rightmost column may be included to the right of the numeric key ‘9’, above the Enter key.

Horizontal layout

The horizontal layout of the command keys shall apply to POS PIN entry devices, where there is insufficient width for a fourth column.

The following specifications apply when the command keys are arranged horizontally:

- The CANCEL key shall be in the leftmost column in the last row
- The ENTER key shall be in the rightmost column in the last row
- The optional CLEAR key shall be placed between the CANCEL and ENTER keys

Depending on the space available on the PIN entry device, the command keys shall be either in:

- the fifth row, below the row containing the ‘0’ key

This arrangement allows the PIN entry device to have at least three command keys: CANCEL, CLEAR and ENTER. This is the recommended horizontal keyboard layout.

- or the same row containing the ‘0’ key

This arrangement allows the PIN entry device to have only two command keys: CANCEL and ENTER. This layout should only be used if there is no space in the PIN entry device to have a fifth row.

Where the PIN entry device does not have a CLEAR command key, the CANCEL key will either clear the current input, or cancel the transaction when there is no input to clear.