



EPC343-08
Version 1.4 approved

30 September 2009

PRIVACY SHIELDING FOR PIN ENTRY

© European Payments Council. [February 2009]
Avenue de Tervueren, 12, 1040, Brussels.

Not to be copied without attribution, and subject to the restriction under the confidentiality clause below.

Comments or enquiries on the document may be addressed to the Secretary General at the above address.

<p>This Implementation document is public, and may be copied or otherwise distributed provided the text is not used directly as a source of profit.</p>



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 during the past years. This new version is now published with an EPC cover page and new number.

This new version is an update of DIG114 v1.0; the introduced changes aim to improve the clarity and to remove redundancy. The introduction, references and definitions have been updated and the scope improved. The most obvious visible changes are to the Figures - these have been reduced in number to avoid duplication and inconsistency, but the fundamental principles remain the same. The most significant change is the reduction of some minimum viewing angles by 5 degrees (from 45 to 40 in certain areas of the shield) in order to align with PCI PED. The reference plane against which protection angles are measured is now either the horizontal plane (for horizontal installations) or the vertical plane (for vertical installations) and is no longer the PIN pad plane. Readers are given a better description of PIN-pad layouts which differ from the norm because, for instance, the function keys are further than usual from the number pad.

There is also greater clarity on how the principles are applied to horizontal and vertical keypads and those at an angle. Whilst much of the text has changed to a greater or lesser degree, the basic principles and approach have not, with the exception of the viewing angle as described above. Devices that could be claimed to have met the previous requirements should not be disadvantaged by the new version.

TABLE OF CONTENTS

1	INTRODUCTION	4
2	REFERENCES AND DEFINITIONS.....	5
2.1	References	5
2.2	Definitions and Abbreviations	5
3	SCOPE AND BACKGROUND.....	7
3.1	Scope.....	7
3.2	Background: PCI and National Requirements	7
4	PRIVACY SHIELDING REQUIREMENTS	8
4.1	General Privacy Shielding	8
4.2	Physical Privacy Shielding Requirements	8
	<i>4.2.1 Basic Concepts</i>	8
	<i>4.2.2 Horizontal Installation</i>	10
	<i>4.2.3 Vertical Installation</i>	11
4.3	Shielding Requirements for Specific Devices and Environments	12
	<i>4.3.1 Handheld Devices</i>	12
	<i>4.3.2 ATMs</i>	12
	ANNEX A: ADDITIONAL ISSUES RELATING TO PRIVACY SHIELDING	13
i.	General Considerations.....	13
ii.	Placement of the PIN Pad.....	13
iii.	Positioning of the PIN Pads for POS Terminals	13
iv.	Cashier and Cardholder Awareness	14

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 Framework 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 the required standardization activities and may be used by banks and banking organisations in discussions with terminal suppliers.

2 REFERENCES AND DEFINITIONS

2.1 REFERENCES

The following documents and papers have been reviewed in the preparation of these standards implementation recommendations:

- CEN TS (Technical Specifications), *Identification card system – Guidance on design for accessible card-activated devices* (prCEN/TS 15291:2006).
- Chip and PIN Programme, UK, *Programme Guideline G16 – Privacy Shields*, version 1.1 (17 February 2004) see also www.chipandpin.co.uk
- CIBEV Werkgroep GEA Certificatie, Dutch Interbank Specifications: *ATM Requirements*, Version 2.2, (November 2004)
- EBS100 Version 3 *Keyboard Layout for ATM and POS PIN Entry Devices* (October 2004)
- 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*
- Payment Card Industry (PCI)¹, *POS PIN Entry Device, Derived Test Requirements, Appendix A – Criteria for the Privacy Screen Design, Version 2.0 (April 2007)*
- PBS, Denmark, *Open Terminal Requirement Specification, Attachment H: Privacy Shield on PIN Entry Devices*, Version 2.2.1 (2 April 2003)
- ZKA, Germany, *Requirements for the assessment of privacy shields in PIN pads*, Version 1.0 (April 2004)

2.2 DEFINITIONS AND ABBREVIATIONS

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

¹ At the time of publication of the present EPC document, PCI has initiated a new PCI PIN Transaction Security program (PTS). Future updates of the EPC PIN shielding document will be done as deemed necessary in view of any upcoming new deliverables from this program.

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 tentative
Observer	A person or device that attempts to discover the PIN by observation
PCI	Payments Card Industry: the group of international card payment schemes who together form the Payment Card Industry Security Standards Council
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
POS	Point of sale (as used in ISO 9564-1) or point of service (as used in EMV 4.2 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

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 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 other members of the public, 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 – the chip and PIN Programme (United Kingdom), the ZKA requirements (Germany) and the PBS requirements (Denmark). 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, as defined in EBS100 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.
- The shield should be considered an integral part of the total design of the terminal/device.
- The shield design needs to allow for use by both right-handed and left-handed cardholders, with a variety of typical hand sizes.

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.

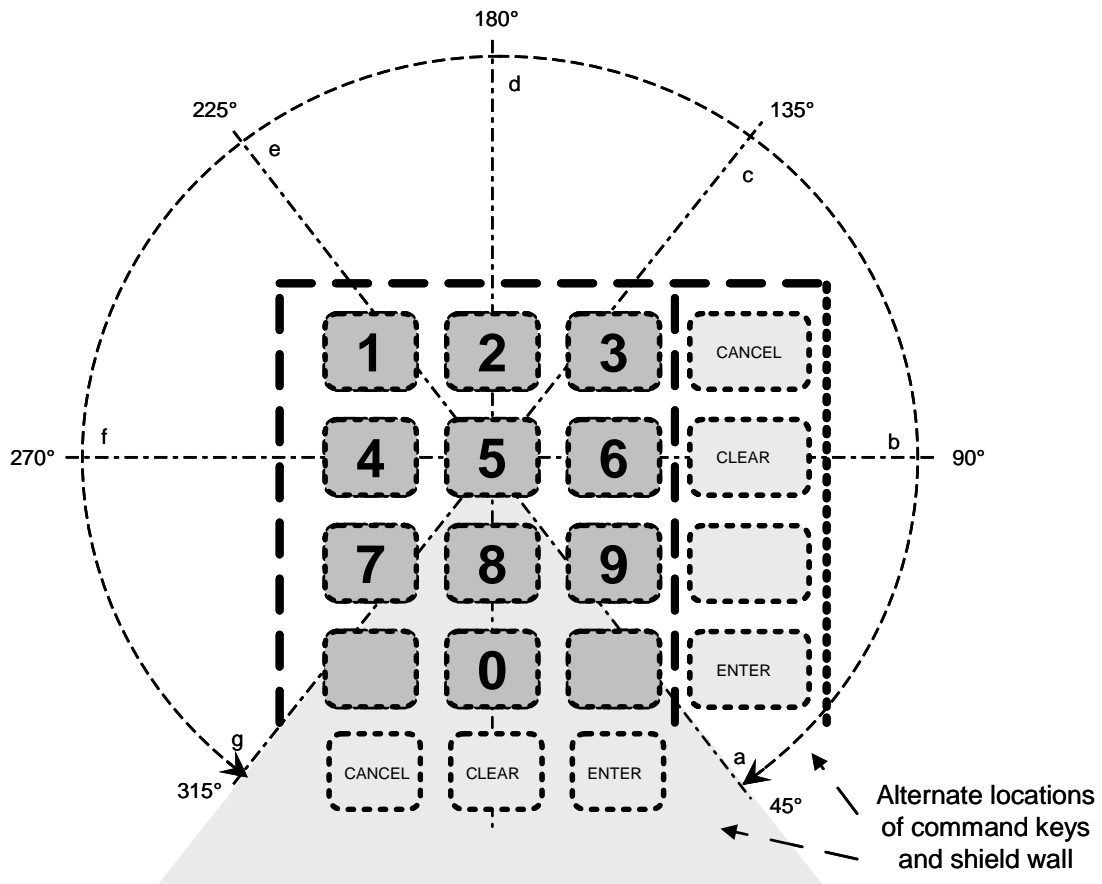


Figure 1: The Reference Point and Protection Zone

Figure 1 illustrates the Reference Point for both the vertical and horizontal layout defined in EBS100 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.

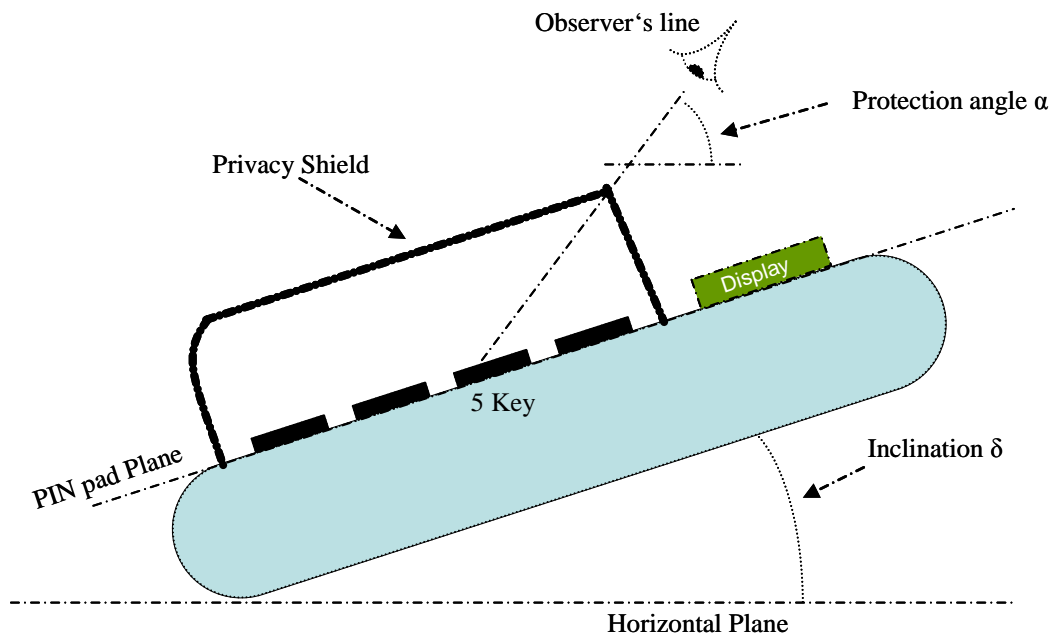


Figure 2: Illustration of the basic concepts (for horizontal installations)

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 (≤ 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**² of the privacy shield is determined by a ray from the Reference Point 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.

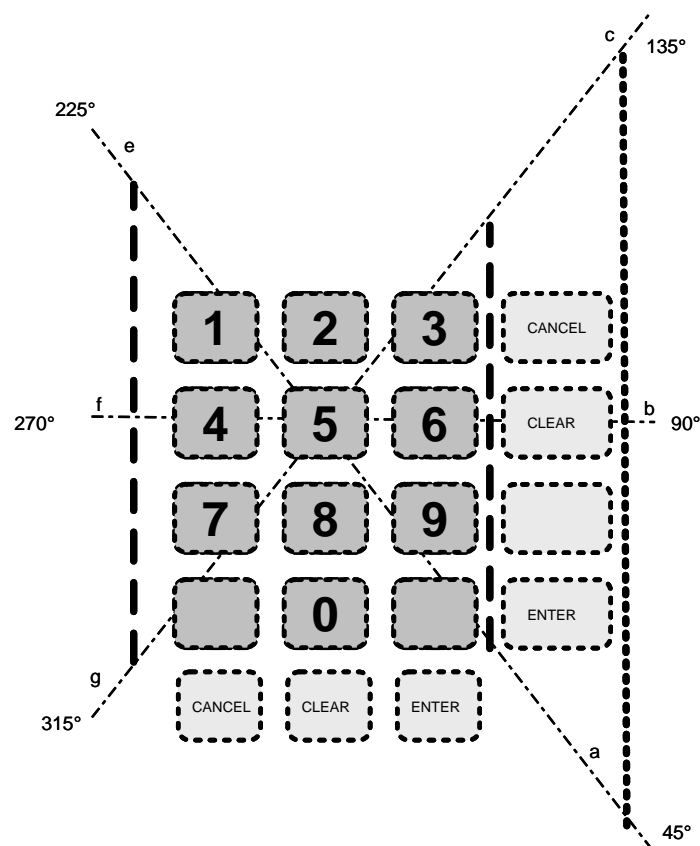


Figure 3: Length of the shield for a vertical installation

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.

² The same terminology is used as for horizontal installations, although shields for vertical installations extend forwards, rather than upwards.

The shielding requirements for vertical installations are primarily intended to protect 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 consideration should be given to continuing the shield around the top of the keypad. 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.

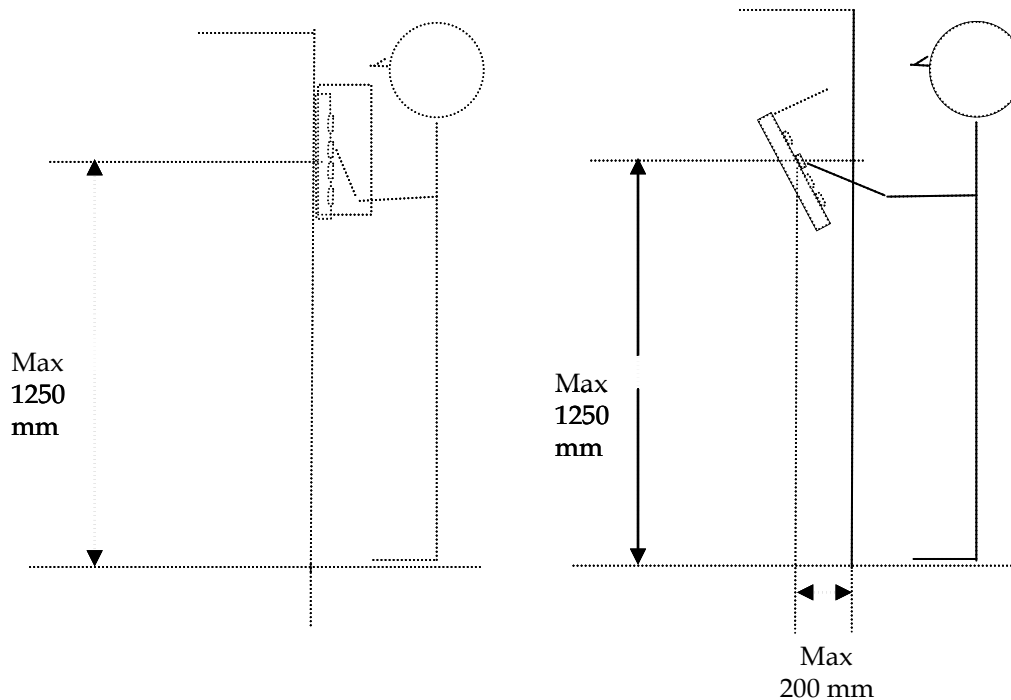


Figure 4: Examples of privacy shielding on vertical installations - keypad on the surface and keypad embedded in the housing of the terminal

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.

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 keyboard.

5 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 Figure 5).
- 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

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 G 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.

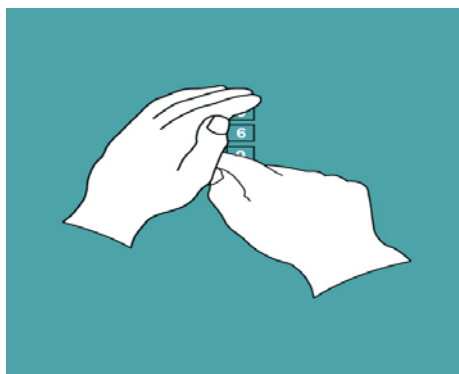


Figure 5: Alert sticker to encourage cardholders to protect their PIN entry