USER MANUAL

SmartPIN™ 100
Encrypting PIN Entry Device

CE FC PCI

80060504-001-A
12-20-2006

FCC WARNING STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his expense.

FCC COMPLIANCE STATEMENT

This device complies with Part 15 of the FCC Rules. Operation of this device is subject to the following conditions: this device may not cause harmful interference and this device must accept any interference received, including interference that may cause undesired operation.

CANADIAN DOC STATEMENT

This digital apparatus does not exceed the Class B limits for radio noise for digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de las classe B prescrites dans le Réglement sur le brouillage radioélectrique édicté par les ministère des Communications du Canada.

CE STANDARDS

An independent laboratory performed testing for compliance to CE requirements. The unit under test was found compliant to Class B.

LIMITED WARRANTY

ID TECH warrants to the original purchaser for a period of 12 months from the date of invoice that this product is in good working order and free from defects in material and workmanship under normal use and service. ID TECH's obligation under this warranty is limited to, at its option, replacing, repairing, or giving credit for any product which has, within the warranty period, been returned to the factory of origin, transportation charges and insurance prepaid, and which is, after examination, disclosed to ID TECH's satisfaction to be thus defective. The expense of removal and reinstallation of any item or items of equipment is not included in this warranty. No person, firm, or corporation is authorized to assume for ID TECH any other liabilities in connection with the sales of any product. In no event shall ID TECH be liable for any special, incidental or consequential damages to purchaser or any third party caused by any defective item of equipment, whether that defect is warranted against or not. Purchaser's sole and exclusive remedy for defective equipment, which does not conform to the requirements of sales, is to have such equipment replaced or repaired by ID TECH. For limited warranty service during the warranty period, please contact ID TECH to obtain a Return Material Authorization (RMA) number & instructions for returning the product.

THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE. THERE ARE NO OTHER WARRANTIES OR GUARANTEES, EXPRESS OR IMPLIED, OTHER THAN THOSE HEREIN STATED. THIS PRODUCT IS SOLD AS IS. IN NO EVENT SHALL ID TECH BE LIABLE FOR CLAIMS BASED UPON BREACH OF EXPRESS OR IMPLIED WARRANTY OF NEGLIGENCE OF ANY OTHER DAMAGES WHETHER DIRECT, IMMEDIATE, FORESEEABLE, CONSEQUENTIAL OR SPECIAL OR FOR ANY EXPENSE INCURRED BY REASON OF THE USE OR MISUSE, SALE OR FABRICATIONS OF PRODUCTS WHICH DO NOT CONFORM TO THE TERMS AND CONDITIONS OF THE CONTRACT.

The information contained herein is provided to the user as a convenience. While every effort has been made to ensure accuracy, ID TECH is not responsible for damages that might occur because of errors or omissions, including any loss of profit or other commercial damage, nor for any infringements or patents or other rights of third parties that may result from its use. The specifications described herein were current at the time of publication, but are subject to change at any time without prior notice.

ID TECH
10721 Walker Street
Cypress, CA 90630
(714)761-6368

TABLE OF CONTENTS

Introduction

SmartPIN is a Personal Identification Number (PIN) Entry Device that encrypts a PIN for secure transmission to a POS terminal or similar equipment. The SmartPIN is primarily used in POS applications where a PIN is used for transaction authorization. This document provides the information for installing and using the SmartPIN product. A separate document is available for application support information.

1. Features & benefits

- Ergonomic Unit with an easy to use design
- Keys are a comfortable size and have good tactile feel
- Provides audio Feedback for each keystroke & for Operation alerts
- Telephone layout for number keys & color-coded control keys
- Interaction function keys for application specific functions
- Provides a two lines by 16 character LCD backlit display
- Payment Card Industry (PCI) security certified
- Meets ANSI and ISO standards for a PIN Entry Device (PED)
- Supports DES and TDES encryption algorithms for PIN encryption
- Provides DUKPT Key Management operations
- Tamper evident, tamper resistant, & tamper responsive design
- Application selectable language options for PIN entry prompt

2. Product configurations

The SmartPIN 100 product has four primary configurations, shown below. Additional configurations are possible, such as SmartPIN with metal keys.

Configuration	Model Number	Description
RS232 w/ LCD	IDPA-7026	SmartPIN PED with LCD Display, RS232 interface cable/connector, & power supply
USB w/ LCD	IDPA-7066	SmartPIN Encrypting PED with LCD Display, USB cable/connector
RS232 w/ No LCD	IDPA-7020	SmartPIN PED without LCD Display, RS232 interface cable/connector, & power supply
USB w/ No LCD	IDPA-7060	SmartPIN Encrypting PED without LCD Display, USB cable/connector

3. Terms, Standards & Related Documents

Glossary

ANSI	American National Standard Institute
API	Application Programming Interface
DES	Data Encryption Standard
DUKPT	Derived Unique Key Per Transaction
EMI	Electromagnetic Interference
EMV	Europay, MasterCard, Visa
ESD	Electrostatic Discharge
Host	A PC, terminal, or controller running Application Software
ISO	International Organization for Standardization
JPOS	Java for Retail Point-of-Sale
LCD	Liquid Crystal Display
MAC	Message Authentication Code
MSR	Magnetic Stripe Reader
MTBF	Mean Time Between Failures
OPOS	OLE for Retail Point-of-Sale
PC	Personal Computer or similar hardware device
PCI	Payment Card Industry
PED	PIN Entry Device
PIN	Personal Identification Number
TDES	Triple Data Encryption Standard
USB	Universal Serial Bus

Related Documents

80071504-001 SmartPIN API User Manual

Standards

ANSI X9.8 & X9.24 Key Management Standards
Meets APACS PED standard
Meets ISO 13491 requirements for temper-evident devices
Meets MAC standard ANSI 9.9 (for future operation)

4. Installation

The SmartPIN unit should be installed in a suitable location where the unit's environmental specifications are not exceeded. Extreme heat or cold should be avoided for reliable operation. The SmartPIN unit is waterproof, can be used in outdoor locations. The location should allow convenient access for the customer. The PIN pad keys must be at a comfortable level for PIN entry and units with a display must have the display information clearly readable by the user.

There are two display options. SmartPIN is available as a PIN entry keypad with no display or with a display and three function keys. The selection depends on the application and available machine options. For machines with no information displays, the SmartPIN with an LCD is required for the PIN entry process. Otherwise, the SmartPIN with no LCD is appropriate for machines with a display or monitor.

SmartPIN is mounted through a bulkhead such that the unit is located on the "safe" side of the bulkhead. The gasket, included with the unit, should be used to seal SmartPIN against the mounting surface. Use internal studs or through bolts with tamperproof heads to secure the SmartPIN body. See Appendix E for dimension information. Some installations may need a keypad shield to prevent observation of the keys pressed for a PIN entry process. This shield may be required for PCI certification of a machine where the SmartPIN is installed. See Appendix F for additional information.

Detailed drawings can be furnished by contacting ID TECH Customer Service. Visit www.idtechproducts.com for contact information.

There are two communication options. The SmartPIN unit can support both RS232 and USB. The communication option is determined by the cable type used. The cable type is factory installed and is not a field selection option.

RS232 Configured Units

Connect the DB9-RS232 connector into the Host equipment communication port. An A/C power adaptor is required to supply power to the RS232 configured unit. To apply power to the unit, first connect the output connector of the power adaptor into the housing of the DB9 (RS232) connector. Then, plug the power supply module into a wall power receptacle to power up the unit.

WARNING: The power adaptor can have input (wall) voltage limitations; DO NOT install a 120VAC power adaptor into a 240VAC wall receptacle.

USB Configured Units

Plug the USB connector into a USB communication port on the Host. No A/C power adaptor is needed to power up the USB unit. The power is supplied by the USB connection. When the USB connector is installed into the Host, power is applied.

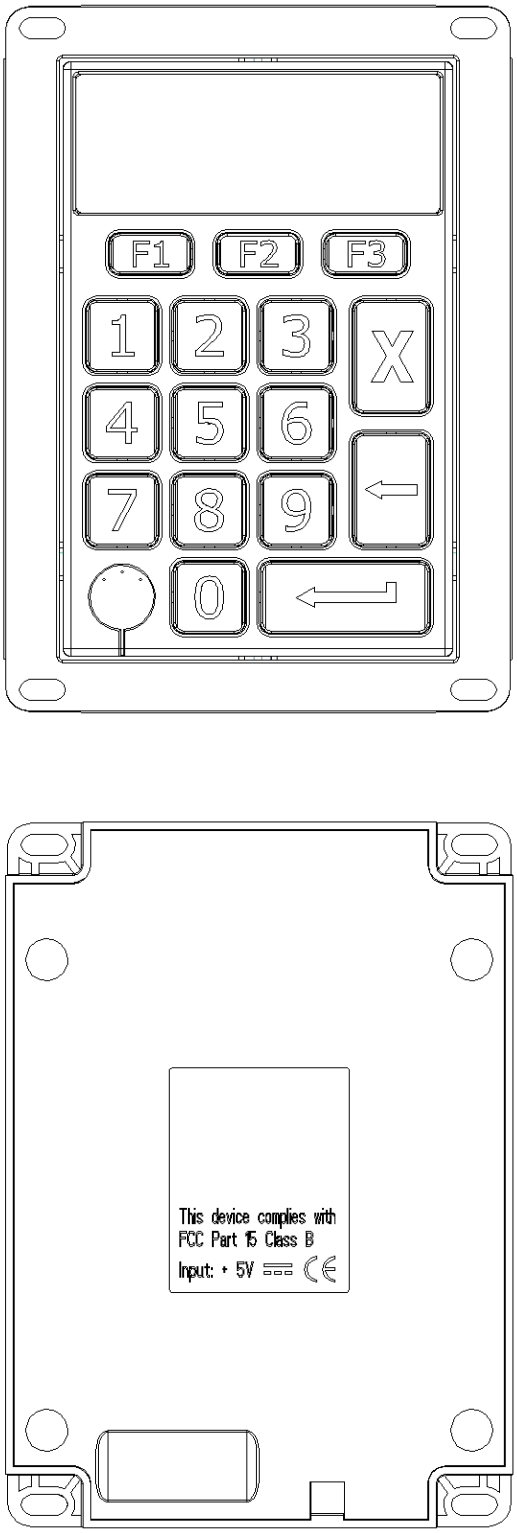


Figure 1 - SmartPIN Features with LCD

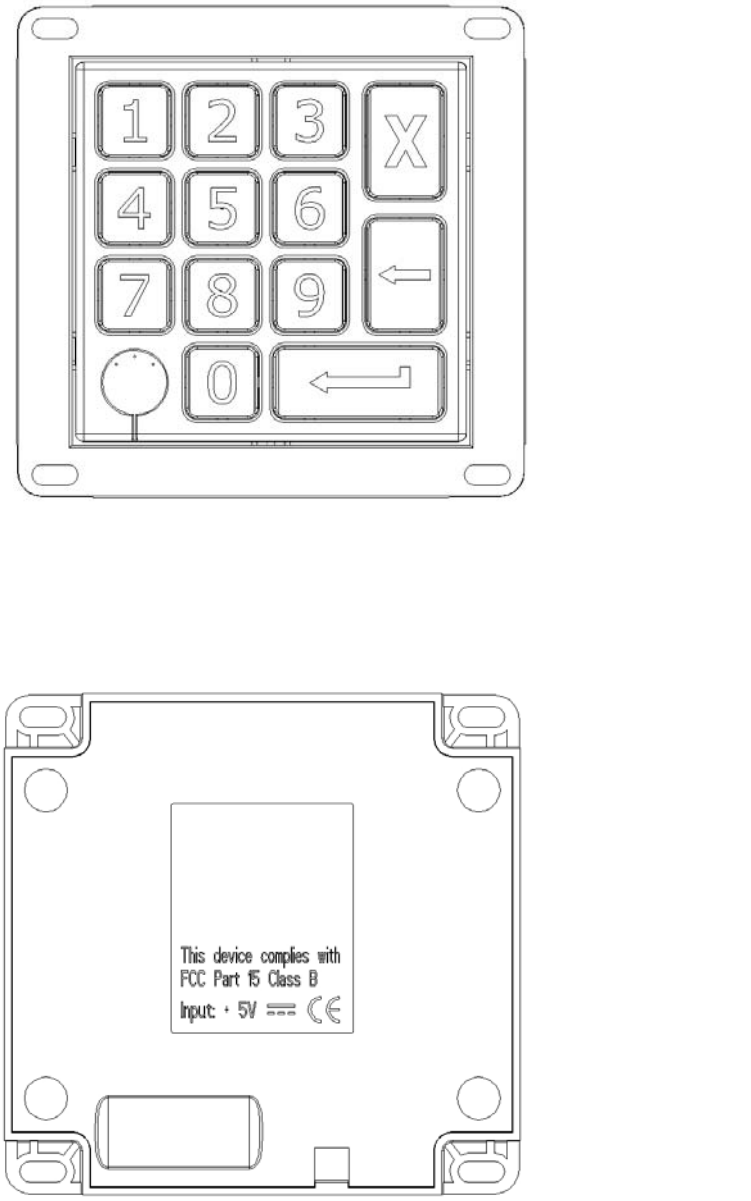


Figure 2 - SmartPIN Features without LCD

5. Operation

General

All units are operated through a POS application command & response (API message) structure. The POS application runs on terminal equipment, a PC, or similar device. Commands cause SmartPIN operations; the SmartPIN provides command responses back to the POS application. Responses are results from commands and can include data. No commands or operations infringe on security requirements. The PIN entry operation is independent to the SmartPIN unit. The PIN entry mode can be initiated and terminated by a POS application command. The full command and response protocol operations are provided in a separate document "SmartPIN API Manual".

Power-Up Sequence

Each time power is applied to the SmartPIN, the unit performs a Power-Up sequence that includes a self-test. During the Power-Up sequence, the display will respond with a message. This is an indication of a successful self-test. For a short period, the Power-Up display will show the model number in the top line and the firmware version number in the bottom line of the display. Finally, the SmartPIN enters and rests in an Idle State.

There are several selectable operations available immediately when the Power-Up display appears; see the appropriate sections in this manual for details on selectable operations.

Operational States

There are three basic Operational States: Idle, PIN Entry, and Transaction.

- The SmartPIN rests in an Idle State when not in use. The display will show "Ready" or a similar application specified message. There is an available power saver mode in the Idle State when enabled by the application software.
- When the POS application sends a get-PIN command to SmartPIN, the unit will transition into a PIN Entry State. The unit operates independently from the Application while in this state. The display message requests a PIN entry. All interactions are between the SmartPIN unit and the operator. The POS application can send a command to cancel the PIN entry process at any time.
- The Transaction State provides operator interactions and information to conclude the transaction. When the transaction is completed, the SmartPIN will again rest in the Idle State.

Audio

There is an audio output device providing a single tone audio feedback for key press recognition. The audio output device can also produce a timed, single tone sequence to alert an operator of a special event. The numeric keys are not operational except during a PIN Entry process. Audio feedback for the numeric keys is provided only during the PIN Entry process.

The audio output can be disables for all functions. The disabled mode can be selected by the POS application or by a key sequence on the unit. See Operation Selections below.

Operation Selections

There are three User Operation selections on the SmartPIN keypad. These functions can be disabled (locked out) by the POS application software. When this feature is not locked out, the unit can be put into the selection mode by pressing the F3, Backspace, and F2 keys in sequential order. This selection mode can be entered at any time the unit is in the Idle State.

When in the Operation Parameters mode, three parameters can be set:

Audio enabled:	On or Off
Backlight enabled:	On or Off
Idle screen prompt:	Selection of installed messages.

There are ten possible stored display messages. The display messages are sent from the POS application and stored in the SmartPIN. These stored messages, together with the factory default messages or a “blank”, can be selected for display on the top line and/or the bottom line of the display. The messages are displayed only when the SmartPIN is in the Idle State.

The F1 (scroll left) or F3 (scroll right) keys are used to display the available selections. Press the Enter key to choose a selection. Press the Cancel key to exit this mode. Each parameter selection can be allowed (enabled or disabled) by the POS application via a command. If any of the selections are not allowed (disabled by the POS application), there will be no display for that selection on the LCD screen.

SmartPIN Operation

Idle Screen

The SmartPIN takes commands from the POS Application through the communication interface. The SmartPIN is typically in an idle mode. In the idle mode, the display will show the selected idle screen display, which is set up by the POS application. The default idle screen shows “Ready” in the top line of the LCD display.

Power Saver Mode

The SmartPIN has a power saving mode. The unit can go into a sleep mode when there has been no operation for a set time. This wait period can be set by the POS application software. The default is no sleep mode (the wait period is set to zero, which disables the sleep mode). If the sleep mode is enabled and the wait period has elapsed, the unit will enter a low power state. SmartPIN will wake up from sleep mode when there is communication from the POS application or when any key is pressed.

For SmartPIN units with an LCD display, the display will be blanked, the backlight turned off during while the unit is in sleep mode.

PIN Entry

Messages are displayed to prompt the user during a PIN entry process. The typical operation is pressing the Number Keys, which correspond to a PIN number, and then pressing the Enter Key to send the PIN in an encrypted format to the POS application software.

During the PIN entry process, there are several options.
To exit the PIN entry process when no digits are entered, press the Cancel Key.
To clear all entered digits and re-start from beginning, press the Cancel Key.
To complete the PIN entry process, press the Enter Key.
To clear the last entry, press the Backspace Key.

For security reasons, the SmartPIN has the following operating functions:

The application can control the overall PIN entry time by issuing commands to enter and then cancel and exit the PIN entry mode. The application may cancel the PIN entry mode for any reason. Once the PIN entry mode is canceled, the PIN entry process must be started from the beginning.

Each PIN digit must be entered within 20 seconds maximum of the last PIN digit. If this time has expired, all the digits entered will be cleared and the time restarted.

The PIN entry process must be completed within 3 minutes maximum. The 3 minutes is timed, starting either from when no PIN characters are entered or from the PIN entry being cleared. When the 3 minutes have expired, the PIN entry process will be automatically canceled.

The SmartPIN has a fixed limit to the number of PIN digits that can be entered. When more than the limit of PIN digits is pressed or a function key is pressed during the PIN entry state, three audio beeps are sounded to signal the input error. No audio beeps are sounded if the audio function is disabled. The limit is set by the POS application software.

6. Maintenance

There are no serviceable components in the SmartPIN. Maintenance is limited to periodic cleaning of the unit to remove oils and dirt.

To clean the unit, use a soft cloth moistened with warm water and a small amount of mild detergent. Disconnect or remove power from the unit and wipe the exterior with the moistened cloth. Caution should be used not to saturate the any area, which would permit liquid to enter the unit. Wipe the unit only enough to clean the surface oil and dirt.

Back up battery

The battery provides power to maintain the contents of cryptographic keys while power to the unit is off. The battery is not intended to power-up the unit into an operational state for any circumstance. The battery is not in use when the unit is powered by an external source. The shelf life of the battery is 3 years minimum total time when no power is applied.

7. Troubleshooting

Power-Up Display

This section is only for SmartPIN with an LCD display. When power is applied, the LCD display will show the model number in the top line and the firmware version number in the bottom line of the display. This information will be shown for about 5 seconds. During this Power-Up display time, the Configuration Display mode or the Diagnostics mode can be selected. These modes are operational from the SmartPIN keys and display. See the Configuration and Diagnostics Mode sections for functional and operational details.

The information from these modes can help in diagnosing operational problems. The RS232 settings must match the Host equipment communication settings.

Configuration Display Mode

Units without a display can be only be configured through the host application software. The unit will go to the Configuration Display mode when the F1 key and then the Enter key are pressed during the power-up display time. The unit setting information will be displayed when in this mode. The RS232 communication settings are shown only for RS232 units and settings related to both the RS232 and the USB units are shown.

Press F1 to scroll up or F3 to scroll down through the parameters.
Press the Cancel key return to idle mode. The unit will return to idle mode if no key is pressed for 15 seconds.

Diagnostic Mode

This section is only for SmartPIN with an LCD display. The unit can be put into a Diagnostic to aid in technical troubleshooting. The Diagnostic mode is entered when the "F1" key and then the "backspace" key are pressed during the power-up display time.

There are three tests that can be selected. They are "audio test", "LCD test" and "keypad test". Press the F1 to scroll up or F3 to scroll down through the test options.

Press "Enter" key to enter the test selected.
Press "Cancel" key to return to idle mode.

The Audio Test will play an ascending and then descending octave and then return to the test selection screen.

The LCD Test displays "LCD Test" for about 2 seconds and then all the display elements will be "on" for about 3 to 4 seconds. Finally, the LCD display advances through the process of showing all supported LCD characters. The unit returns to the test selection screen when all the characters are displayed or if any key is pressed while the LCD is displaying characters.

The Keypad Test will show the key designation on the LCD display when any key is pressed. The Enter key is shown as "E" and the Backspace key is shown as "B". Pressing the "Cancel" key will return the unit back to the test selection screen.

If no selection is made within 15 seconds, the unit will return to the idle mode.

Appendix A Specifications

Power Requirements

Power is supplied to the unit in the following manner:
RS232C interface - A/C power adapter, 5VDC +/- 10%
USB interface – Hub supplied power is less than 250mA

Encryption & Key Management

Employs DES and TDES encryption algorithms

DUKPT key management

Operating Environment

Temperature Range

Operating:	Indoor: 5 to 40° C (41 to 104° F)
	Outdoor: -10 to 55° C (14 to 131° F)
Non-operating:	Indoor: 0 to 60° C (32 to 140°F)
	Outdoor: -20 to 70° C (-4 to 158° F)
Shipping:	-20 to 70° C (-4 to 158° F)

Relative Humidity Range (non-condensing)

Operating	8 to 95 % with Wet bulb at 23°C (73.4°F)

Electromagnetic Interference (EMI)
FCC part 15 Class B
CISPRA B

Communication Interface

RS232 or USB-CDC

Mechanical with LCD

Dimensions:

Height 32.8mm (1.29")
Width 95.0mm (3.74")
Length 138.0mm (5.43")

Keys:

Indoor: Hard rubber material, Numeric (10), Function (3), Control (3)
Outdoor: Metal material, Numeric (10), Function (3), Control (3)

Display:

2 x 16 Character back lighted LCD

Mechanical without LCD

Dimensions:

Height 32.8mm (1.29")
Width 95.0mm (3.74")
Length 96.0mm (3.78")

Keys:

Indoor: Hard rubber material, Numeric (10) & Control (3)
Outdoor: Metal material, Numeric (10) & Control (3)

Reliability

Electrostatic Discharge (ESD)

Units will withstand minimum 4KV direct contact and 8KV electrostatic air discharge without resetting.

Drop Test:

Withstands 3 ft drop to concrete, 6 surfaces & 4 corners
No functional damage

MTBF Minimum calculated MTBF value of 160,000 power on hours.

Appendix B Communication Parameters Table

Following table provides a list of settings that can be set. The settings are initialized to the factory default setting is shown in bold type. The POS application can modify the settings to suit the application requirements.

RS232 communication settings:
Baud rate:
1200 bits/second
2400
4800
9600
14.4K
19.2K
28.8K
38.4K
57.6K
115.2K
Number of data bits
7
8
Number of stop bits
1
2
Parity
None
Odd
Even
General Settings:
Sleep (time out period):
0 second – never timed out
1 to 240 seconds
Audio control
On
Off
Backlight control
On
Off

Appendix C Language Options Table

Only for SmartPIN with an LCD display.

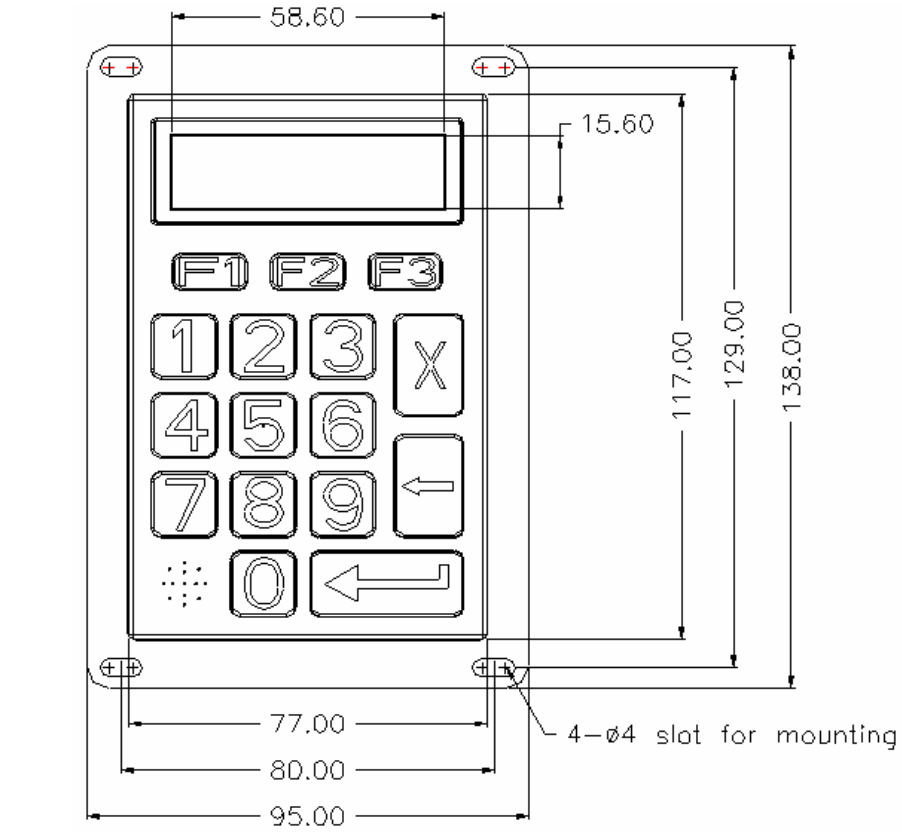
Language type	PIN Request	Ready Display
English	Enter PIN	Ready
French	Code?	Prêt
German	Geheimnummer	Bereit
Italian	Entri PIN	Preparato
Portuguese	Digite Senha	Pronto
Spanish 1	Entrad Clave	Preparado
Spanish 2	Entrad PIN	Preparado
Other	PIN ??	Prepared

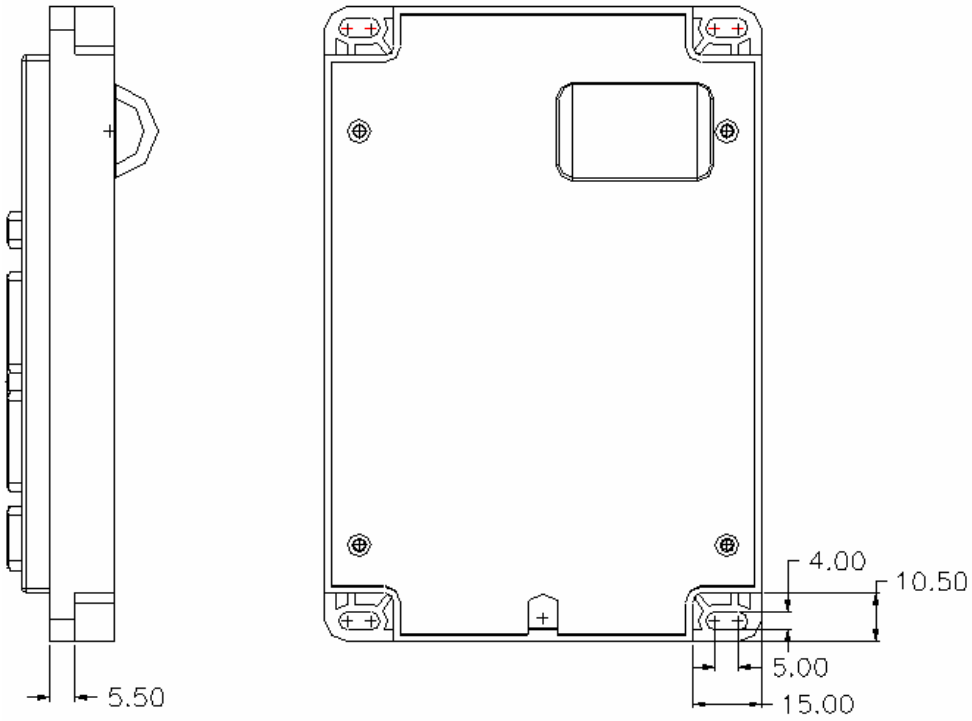
Appendix D Message Explanations

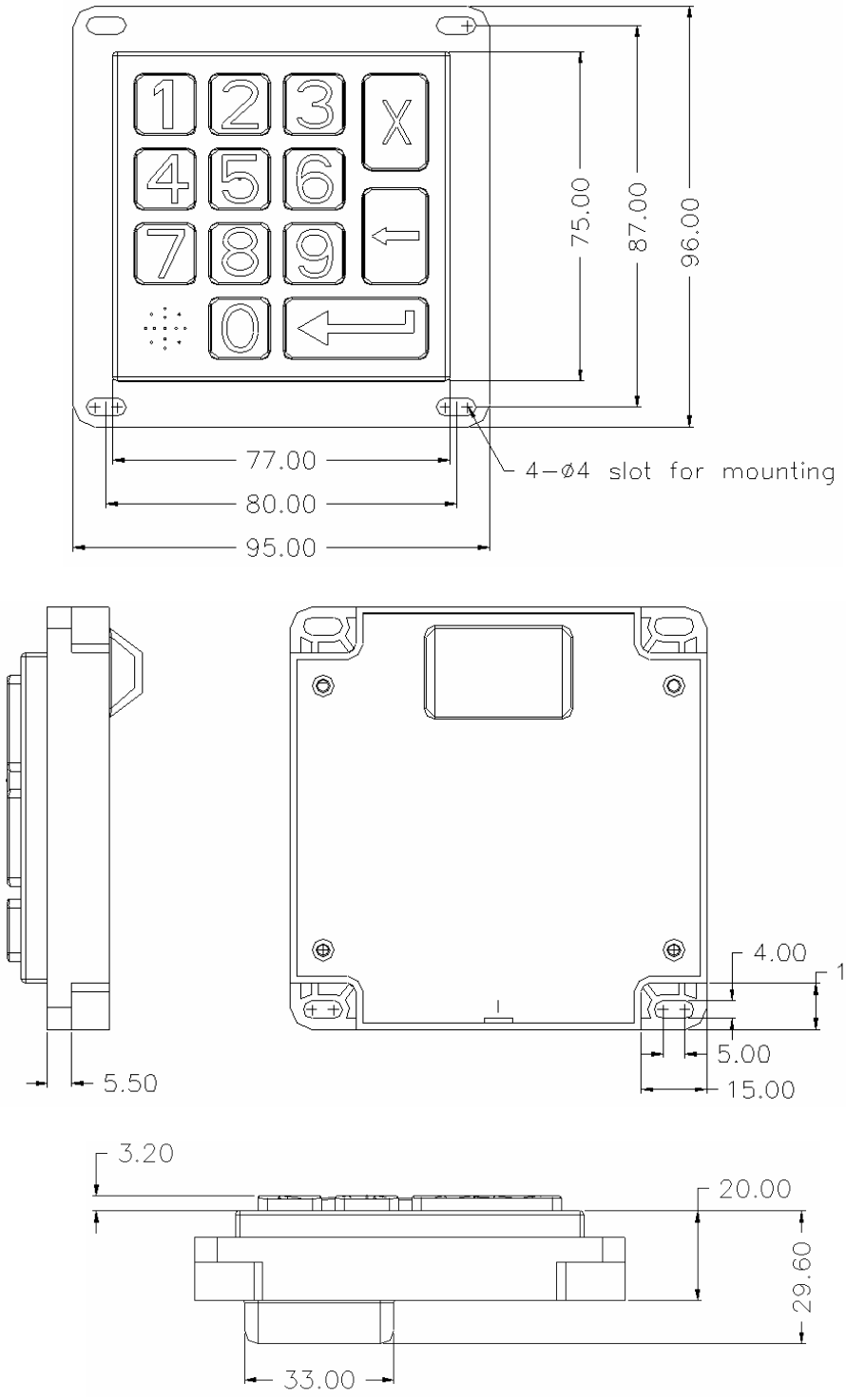
There are messages not shown in normal operation. The message and the meaning are given in the table. *These messages are shown only on SmartPIN with an LCD display.*

Message	Explanation
FATAL ERROR Repair Unit	Error message when unit is not activated in the manufacturing or key injection process or when the unit has been physically compromised. The unit is in a "locked-up" mode and must be returned for repair or discarded.
Unit Suspend	Warning message during the time the unit has been locked-up due to too many PIN entries in short intervals
Warning	This is a warning message for Checksum errors or for battery failure. The second line of the display indicates which of the two is at fault. The unit is in the locked-up mode and must be returned for repair or discard.
Checksum Err	A communication check sum does not match
No Battery	A battery failure indication

Appendix E Outline Drawings







Appendix F Privacy Shield Installation

In order to meet PCI security requirements, a “privacy” shield must be designed and installed together with the SmartPIN in the final system installation. This section provides the design criteria to be used for implementing a privacy shield when installing the SmartPIN in a PCI application

The following sections show how the privacy shield can be installed and define the requirement for the shield(s).

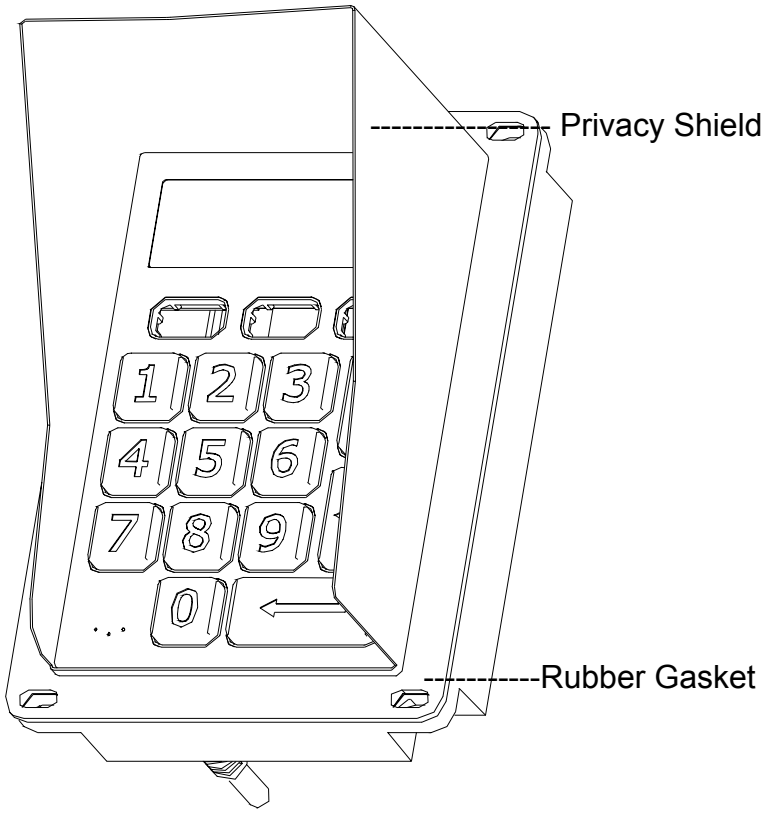


Figure 3A: Privacy shield relative to Keys & faceplate, SmartPIN with LCD

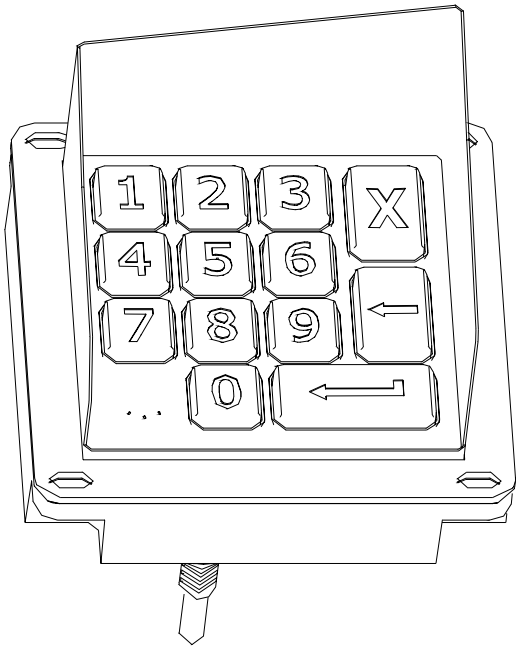


Figure 3B: Privacy shield relative to Keys & faceplate, SmartPIN without LCD

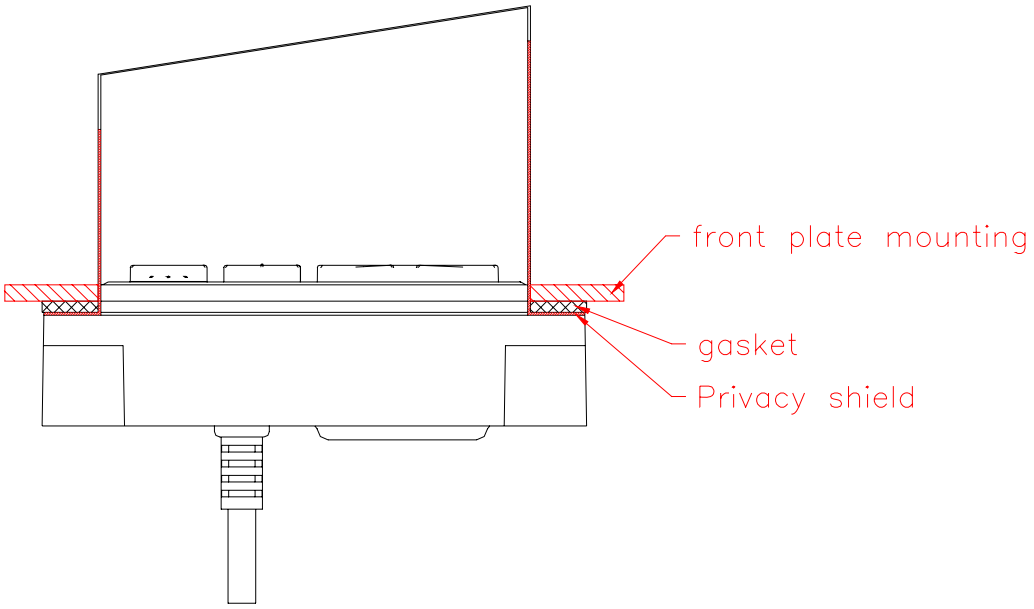
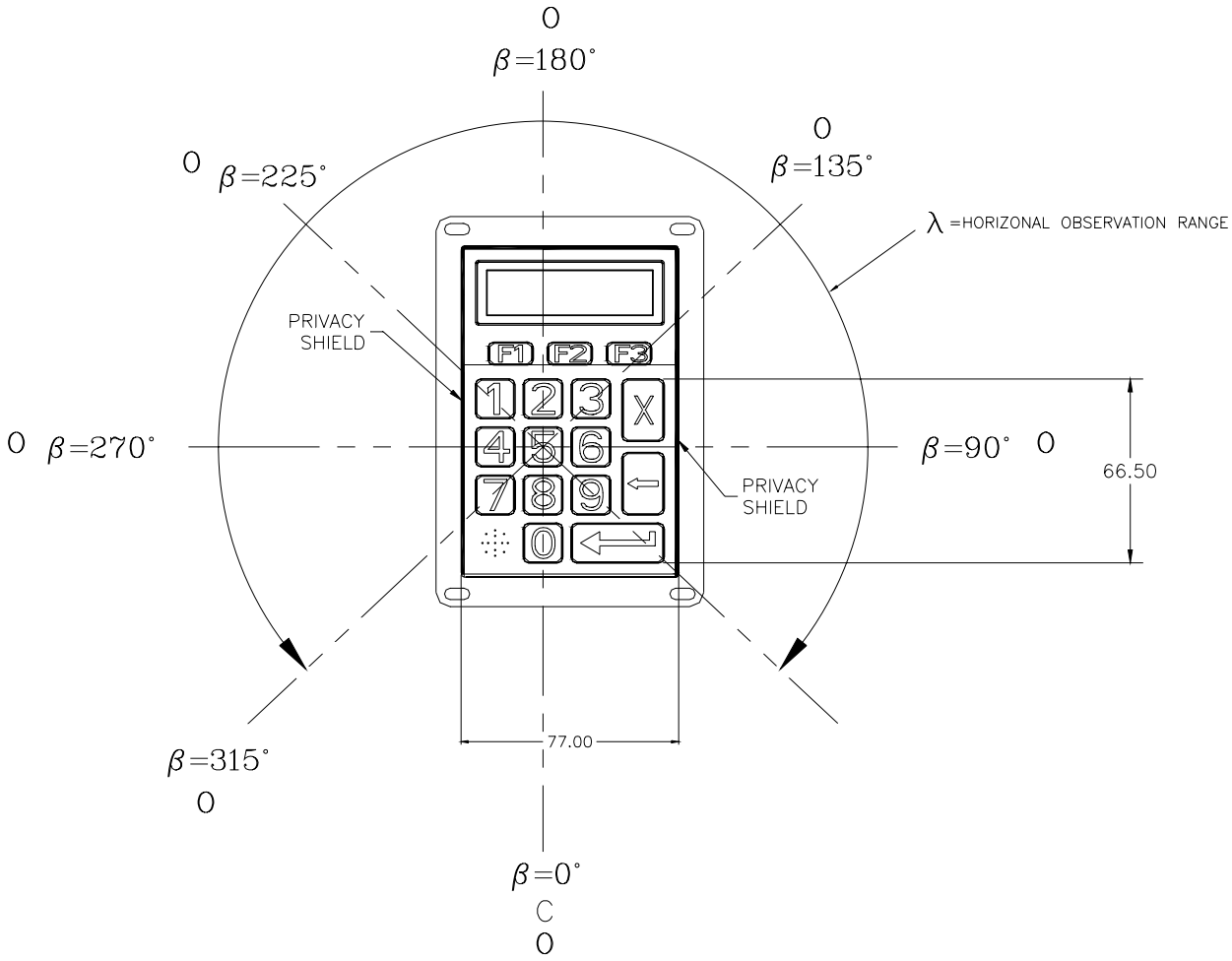


Figure 4: Method for securing privacy shield under the mounting plate and sealing gasket

Design Criteria for Privacy Shielding

The following sections define the minimum requirements for determining the amount of shielding needed to meet PCI requirements, All observation points are referenced to the '5' key.



O = Observer
C = PED user (card holder)

Figure 5: Sample SmartPIN with privacy shield, bird's eye view

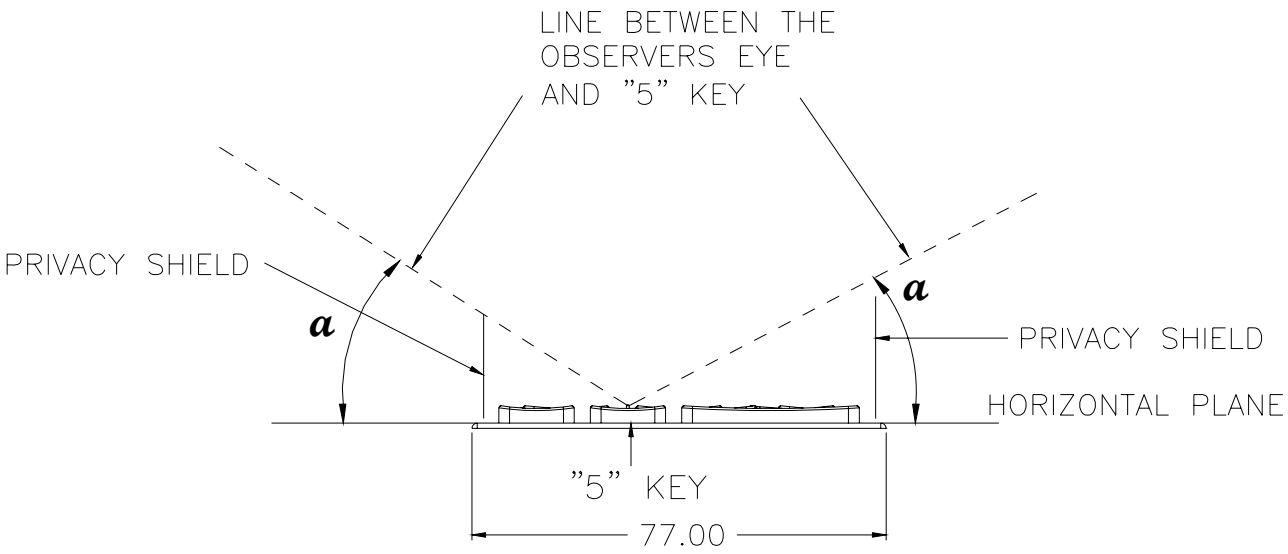


Figure 6: Sample of SmartPIN front side view

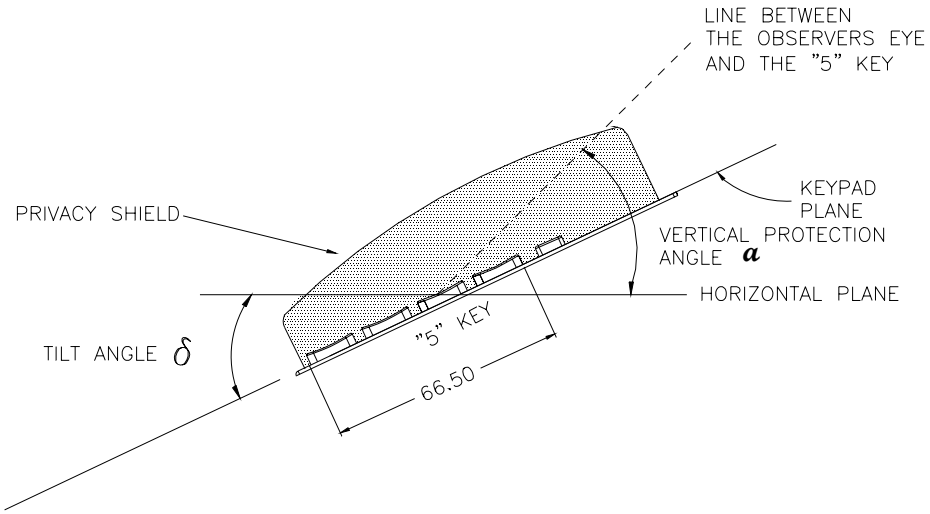


Figure 7: Sample SmartPIN, side view

The angles in figures 5 through 7 are defined as following:

α = Angle between the horizontal plane through the '5' key and virtual line which connects the '5' key and an observer's eye.

β = Horizontal position of an observer relative to the PED user's position

λ = horizontal range which is to be covered by the privacy shield

δ = Angle between the keypad plane and horizontal plane (tilt angle)

Design Rules:

1. The privacy shield is to be placed horizontally or slightly tilted ($0 \le \delta \le 45°$) and shall provide the following protection angles:

Horizontal angle β	Remark	Vertical Angle α
$315° \le \beta \le 45°$	Within this range of β the card holder deters an observer with his/her body	N/A
$45° \le \beta \le 90°$	Within these range visual observation of the keypad is partially blocked by the cardholder	$\alpha \ge 35°$
$270° \le \beta \le 315°$	The protection angle α shall be at least 35°. Please note that the front end of the privacy shield must be higher if the SmartPIN is tilted	$\alpha \ge 35°$
$90° \le \beta \le 270°$	The protection angle shall be at least 40°. The display side of the privacy shield may be lowered as SmartPIN is tilted against the horizontal plane	$\alpha \ge 40°$

The vertical angles given in the table above are with respect to the horizontal plane (see figure 7). If by design SmartPIN is tilted toward the card holder, the backside of the privacy shield may be lower

2. If the SmartPIN is to be placed vertically or tilted by 45° or more, the requirement under step 3 will apply accordingly, using the vertical plane instead of the horizontal plane as the reference for the angle α.

3. The protection is based on viewing angles and does not imply a specific technical implementation like physical shields. If the keypad is implemented as a touch screen, the viewing barrier maybe implemented by polarizer (e.g., as film on the touch screen surface), which deter the observation from the sides. The up (clerk) side must be implemented as a physical shield

The following techniques can be employed to provide for effective shields of the SmartPIN keypad during the PIN entry process. These methods would typically be used in combination, though in some cases a method might be used singly.

Note: This option does not preclude the use of privacy mechanisms as defined in figure 5, but allows less restrictive physical mechanisms, e.g. $\alpha \geq 20°$.

- Positioning of SmartPIN on the kiosk/terminal in such way as to make visual observation of the PIN-entry process infeasible. Example include:
  - Visual shields designed into the kiosk/terminal. The shields may be solely for shielding purposes, or may be part of the general kiosk/terminal design, e.g., used as selling area.
  - Position the SmartPIN so that it is angled in such a way to make PIN spying difficult.
- Positioning of Security cameras such that the PIN-entry keypad is not visible.
- Instruction the cardholder regarding safe PIN-entry. This can be done with a combination of :
  - signage on the kiosk/terminal
  - prompts on the display, possibly with a “click-through” screen
  - potentially literature at the point of sale
  - a logo for safe PIN-entry process

The above methods should be used in conjunctions with the design criteria defined in figures 5 though 7 to provide PCI compliant shielding.