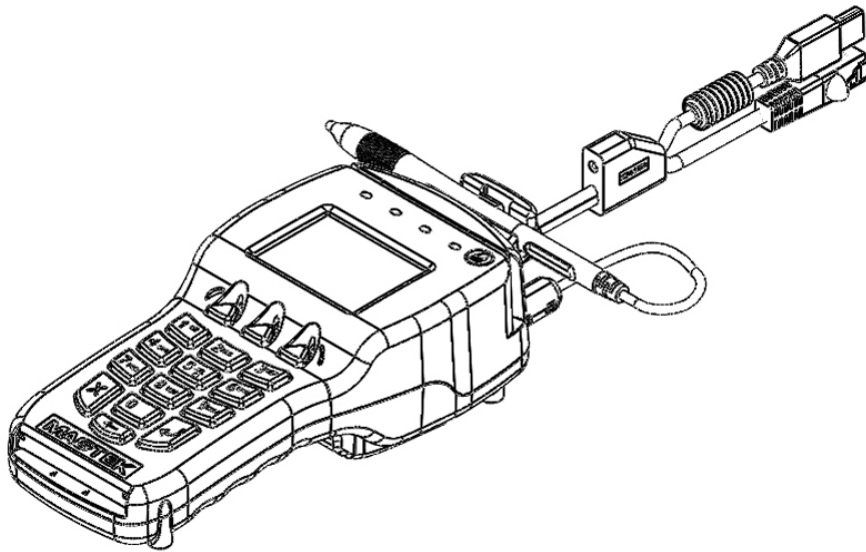


DynaPro

PIN Encryption Device

DynaPro Installation and Operation Manual



October 2013

Manual Part Number:
99875586-3.01

REGISTERED TO ISO 9001:2008

Copyright[©] 2007 - 2012
MagTek[®], Inc.
Printed in the United States of America

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MagTek, Inc.

MagTek is a registered trademark of MagTek, Inc.

MagneSafe[™] is a trademark of MagTek, Inc.

MagnePrint[®] is a trademark of MagTek, Inc.

REVISIONS

Rev Number	Date	Notes
1.01	August 15, 2012	Initial Release
2.01	September 10, 2013	Updates include: changing name from IPAD EMV to DynaPro; including Ethernet and USB descriptions; updated dimensions; updated images; updated formatting.
3.01	October 25, 2013	Updated screens in Section 4 Added Section 4.8 for EMV transaction

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 the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC COMPLIANCE STATEMENT

This device complies with Part 15 of the FCC Rules. Operation of this device is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CUR/UR

This product is recognized per Underwriter Laboratories and Canadian Underwriter Laboratories 1950.

RoHS STATEMENT

When ordered as RoHS compliant, this product meets the Electrical and Electronic Equipment (EEE) Reduction of Hazardous Substances (RoHS) European Directive 2011/65/EC. The marking is clearly recognizable, either as written words like “Pb-free”, “lead-free”, or as another clear symbol ().

Table of Contents

1	INTRODUCTION AND SPECIFICATIONS	1
1.1	Product Description.....	1
1.2	Design Objectives.....	1
1.2.1	Securing Personal Cardholder Data	1
1.2.2	Protection for all Points within the Payment Infrastructure	1
1.2.3	Security and Ease of Integration by Design	1
1.2.4	Greater Flexibility Reduces Total Cost of Ownership.....	1
1.3	Design Features	2
1.4	Major Components.....	3
1.5	Specifications	5
1.6	Pinout on RJ-25 6-pin Connector	6
2	SYSTEM REQUIREMENTS & DEVICE FEATURES	7
2.1	System Requirements.....	7
2.2	Device Features.....	7
2.2.1	Physical and Electronic Security	7
2.2.2	Sleep Mode	7
2.2.3	Liquid Crystal Display.....	7
2.2.4	Function Buttons (Soft Keys).....	7
2.2.5	10-Digit Numeric Pad	7
2.2.6	Magnetic Card Reading	7
2.2.7	ICC Card Reading	8
2.2.8	Contactless Card Reading.....	8
3	INSTALLATION	9
3.1	USB Installation	9
3.2	Ethernet Installation.....	10
3.3	Privacy Shield Installation.....	11
3.4	Privacy Shield Removal.....	11
3.5	Mounting Dimensions	12
4	OPERATION.....	13
4.1	Overview.....	13
4.2	Card Reading using the SCR	14
4.3	Manual Card Entry.....	14
4.4	Selecting the Card Type	15

4.5	PIN Entry	15
4.6	Amount Verify	16
4.7	Signature Capture	16
4.8	Card Reading using the Smartcard Reader for an EMV Transaction	17
4.9	Status Codes	19
5	MAINTENANCE	20
5.1	Cleaning	20
5.2	Adjusting the LCD	20

FIGURES

Figure 1-1. DynaPro USB and ETHERNET	2
Figure 1-2. Major Components (front)	3
Figure 1-3. With Privacy Shield.....	3
Figure 1-4. Major Components (back)	4
Figure 1-5. RJ25 6-Pin Connector	6
Figure 3-1. USB Interface	9
Figure 3-2. Ethernet Interface	10
Figure 3-3. Installing the Privacy Shield	11
Figure 3-4. Mounting Dimensions and Cable Access Hole.....	12
Figure 4-1. Example of Welcome Screen (Ready for a New Transaction)	13
Figure 4-2. Example of Swipe Card Screen	14
Figure 4-3. Example of User Screen to Manually Enter Card Data	14
Figure 4-4. Example of User Screen to Select Card Type	15
Figure 4-5. Example of User Screen to Enter PIN	15
Figure 4-6. Example of User Screen to Verify Amount.....	16
Figure 4-7. Example of User Screen to Enter Signature	16
Figure 4-8. Example of EMV card insertion	17
Figure 4-9. Processing Screen.....	17
Figure 4-10. Example of Enter PIN Screen for EMV Transactions	18
Figure 4-11. Examples of Screen Approved, Declined or Terminated.....	18
Figure 4-12. Examples of Screen Remove Card	19
Figure 5-1. Adjusting the DynaPro's LCD.....	20

1 INTRODUCTION AND SPECIFICATIONS

1.1 Product Description

The DynaPro is a secure PIN encryption device combined with MagTek's 3-Track MagneSafe™ secure card reader. The DynaPro provides the most comprehensive end-to-end security solution to prevent personal cardholder data breaches while bringing convenience and speed to Retail and Financial transactions.

1.2 Design Objectives

1.2.1 Securing Personal Cardholder Data

The DynaPro immediately encrypts data at the point of swipe to safeguard personal information encoded on the magnetic stripe. The encryption takes place within an encapsulated magnetic read head as the card is swiped, eliminating the chance of intercepting clear text data. The DynaPro's data encryption scheme uses the industry standard TDEA (3DES) algorithm, which offers merchants, processors, issuers and acquirers the flexibility to manage decryption services themselves or to outsource, thereby avoiding the risk imposed by unproven, proprietary encryption algorithms.

1.2.2 Protection for all Points within the Payment Infrastructure

In addition to meeting the requirements established by PCI PTS v3.x, which incorporates SRED features, the DynaPro has MagnePrint®, a proven embedded security feature that authenticates the debit, credit, or gift card and its encoded track data, rendering counterfeit or cloned cards useless. So even if cardholder data is acquired for the purpose of manufacturing counterfeit cards, such cards can be detected, the transaction can be declined, and the criminal can be prosecuted. The MagnePrint feature provides a valuable defense to protect the merchant, the acquirer, the processor, the card issuer, and ultimately the consumer.

1.2.3 Security and Ease of Integration by Design

In addition to securing clear text card data, the DynaPro uses a 32-bit secure processor which incorporates flexible data formatting and masking capabilities for compatibility with existing software and payment applications, eliminating the need for recertification.

The DynaPro supports Device Authentication so the retailer, processor, and acquirer have the confidence of knowing that a rogue reader was not substituted and provides transparency to the processor, acquirer, or ISO if the device is changed. Furthermore, it supports Mutual Authentication through a secure challenge/response sequence, which eliminates both the potential of being redirected to an illegitimate site and the ability to substitute a compromised PINpad terminal.

1.2.4 Greater Flexibility Reduces Total Cost of Ownership

The DynaPro supports secure remote key injection, eliminating the need to return the unit in the event a new key is required.

1.3 Design Features

- PCI PTS v3.x, SRED Compliant
- Meets EMV level 1 and 2 requirements
- 3 Track Secure Card Reader
- Smart card EMV reader
- Contactless reader (optional)
- Backlit color LCD graphics
- Optional real-time electronic signature capture
- Optional privacy shield
- 16-digit key pad
- Connectivity via USB HID or Ethernet
- TDEA (3DES) Encryption
- DUKPT Key Management
- Remote Key Injection
- Card and Data Authentication
- Device Authentication
- Mutual Authentication
- Flexible Data Formats
- Flexible Data Masking

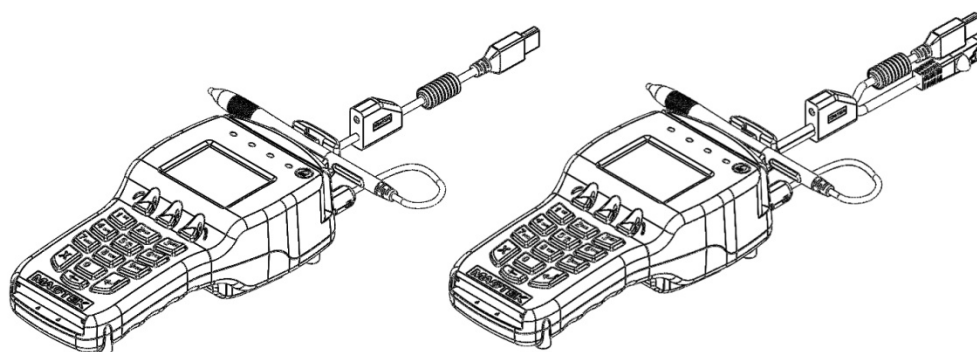


Figure 1-1. DynaPro USB and ETHERNET

1.4 Major Components

The major components of the DynaPro are shown in Figures 1-2, 1-3 and 1-4.

Note: The ferrite bead must remain attached to the stylus cable at all times, do not remove.
Changes or modifications not expressly approved by MagTek could void the user's authority to operate the equipment.

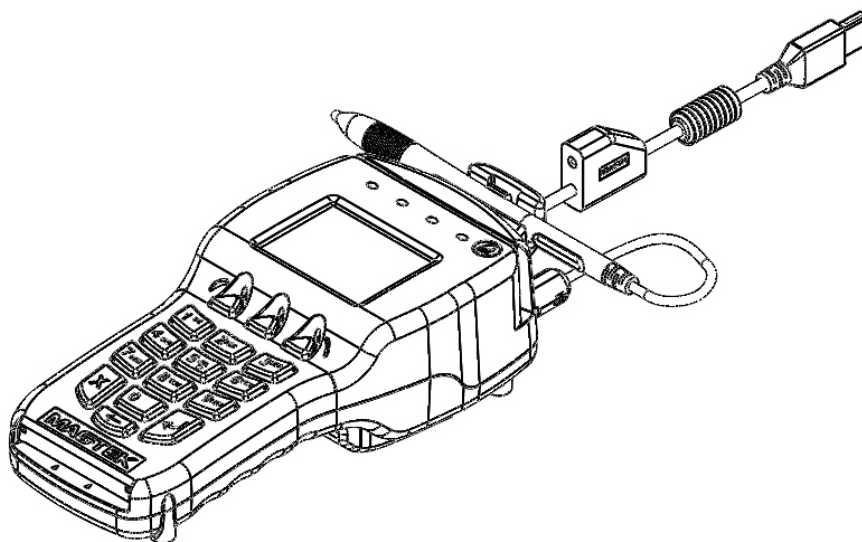


Figure 1-2. Major Components (front)

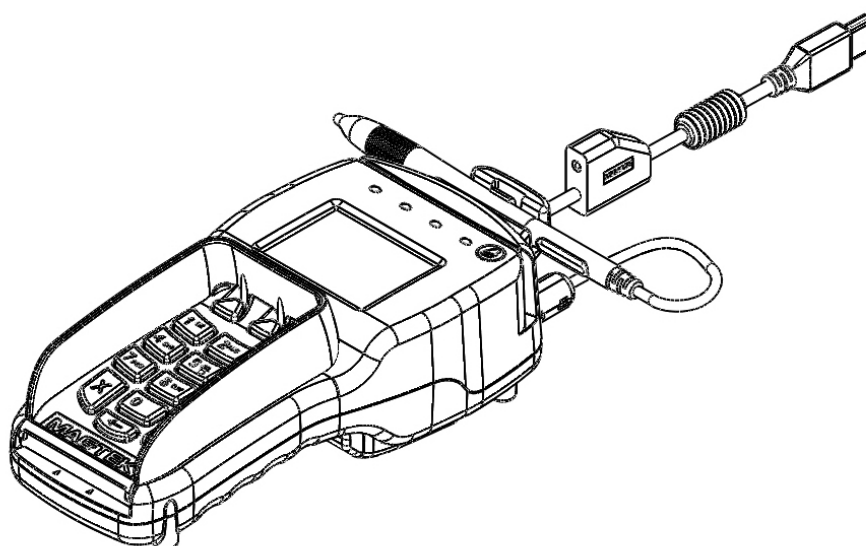


Figure 1-3. With Privacy Shield

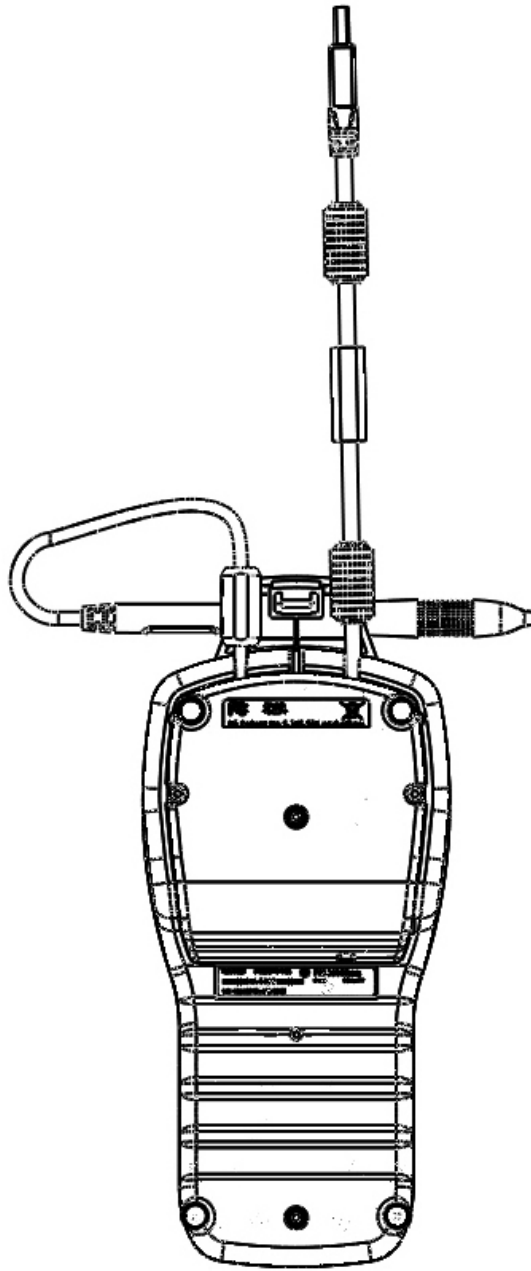


Figure 1-4. Major Components (back)

1.5 Specifications

Electrical	
Power Input:	USB Bus Powered (Power adaptor required for contactless or Ethernet)
Voltage:	5VDC
Current:	250mA (900mA with contactless)
Interfaces:	USB 2.0 (USB 1.1 compatible) and Ethernet
Display Type:	Backlit, color liquid crystal display (LCD)
Display Resolution:	240 x 320 dpi
Flash Memory:	256 MBit
Internal SDRAM memory:	64 MBit
Battery type:	Lithium

Mechanical	
Dimensions (L x W x H):	8.8in x 3.9in x 2.4in (223.5mm x 99.1mm x 61.0mm)
Weight:	1 lb
Keypad:	16-key, includes 3 soft function keys associated with LCD
Cable Length (standard):	6.75 ft (2 m)
Card Reader:	3 track encrypting IntelliHead reader with MagnePrint
Connector Type:	RJ25 modular jack

Environmental	
Temperature:	
Operating:	32 °F to 113 °F (0 °C to 45 °C)
Storage:	14 °F to 140 °F (-10 °C to 60 °C)
Relative Humidity:	
Operating:	10% to 90% non-condensing at 23 °C
Storage:	Up to 90% non-condensing

Reliability	
Expected Life (unit):	1,000,000 card swipes (equivalent to 5 years of operation)
Battery Life:	5 years shelf life

1.6 Pinout on RJ-25 6-pin Connector

RJ25 Connector	Signal
1	VBUS
2	USB_DM
3	USB_DP
4	GND
5	NC
6	CGND

Pin 1

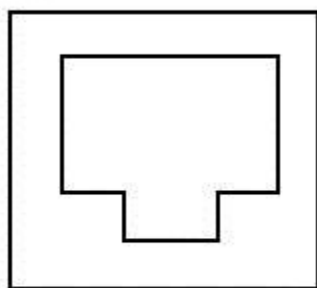


Figure 1-5. RJ25 6-Pin Connector

2 SYSTEM REQUIREMENTS & DEVICE FEATURES

2.1 System Requirements

- Windows XP or later (32-bit or 64-bit)
- Microsoft .NET Framework version 2.0 (Not required but suggested)
- USB port

Upon installation, Windows will automatically recognize and install the USB drivers for this device.

2.2 Device Features

2.2.1 Physical and Electronic Security

The DynaPro enclosure and its associated electronics have been designed to form a Tamper Resistant Security Module (TRSM). The covers are securely attached and incorporate sensing circuits to detect if any attempt is made to open the unit. Internal spaces within the DynaPro have been minimized to reduce the possibility of unauthorized modifications.

In addition, any attempt to penetrate or modify the DynaPro electronically will cause the unit to permanently erase its stored encryption keys, after which the DynaPro will cease to function.

2.2.2 Sleep Mode

When the Windows operating system shuts down or is suspended the DynaPro will enter into a *sleep mode*.

2.2.3 Liquid Crystal Display

The Liquid Crystal Display (LCD) is a color graphics display capable of showing static or animated messages.

2.2.4 Function Buttons (Soft Keys)

The three function buttons or *soft keys* are located below the LCD screen. These buttons are programmable for use with display-based prompts.

2.2.5 10-Digit Numeric Pad

During normal operation the numeric keypad is used for PIN entries. An audio tone will provide feedback when entering the PIN digits. There are three additional keys that may be used during a transaction: an ENTER button (green), a CLEAR button (yellow), and a CANCEL button (red).

2.2.6 Magnetic Card Reading

The DynaPro contains a MagneSafe card reader that encrypts card data at the point of swipe to protect the cardholder's personal information. The reader incorporates MagTek's 3-track encrypting IntelliHead, a magnetic read head which has encapsulated and securely potted electronics that reads, decodes, and encrypts card data within the head. This technology secures the magnetic stripe data at the earliest point in the transaction chain—the initial swipe.

In addition, as a card is swiped through the reader, through the use of MagnePrint technology the card can be authenticated immediately, either by Magensa.net or by another system, to determine whether the card is counterfeit or has been altered.

The card reader is capable of reading any ISO or AAMVA encoded magnetic stripe data.

2.2.7 ICC Card Reading

The DynaPro includes a smart card (ICC) reader. The card is inserted from the front of the unit under the keypad.

2.2.8 Contactless Card Reading

The DynaPro includes an optional contactless card reader. The card is waved above the LCD.

3 INSTALLATION

3.1 USB Installation

To connect the DynaPro to a computer, connect its USB cable to the USB port on the computer as shown in Figure 3-1. Note: the standard USB cable P/N 30019317 is six feet long.

⚠ WARNING

Connecting or disconnecting the USB cable from the back side of the DynaPro when the computer is ON may clear the encryption keys.

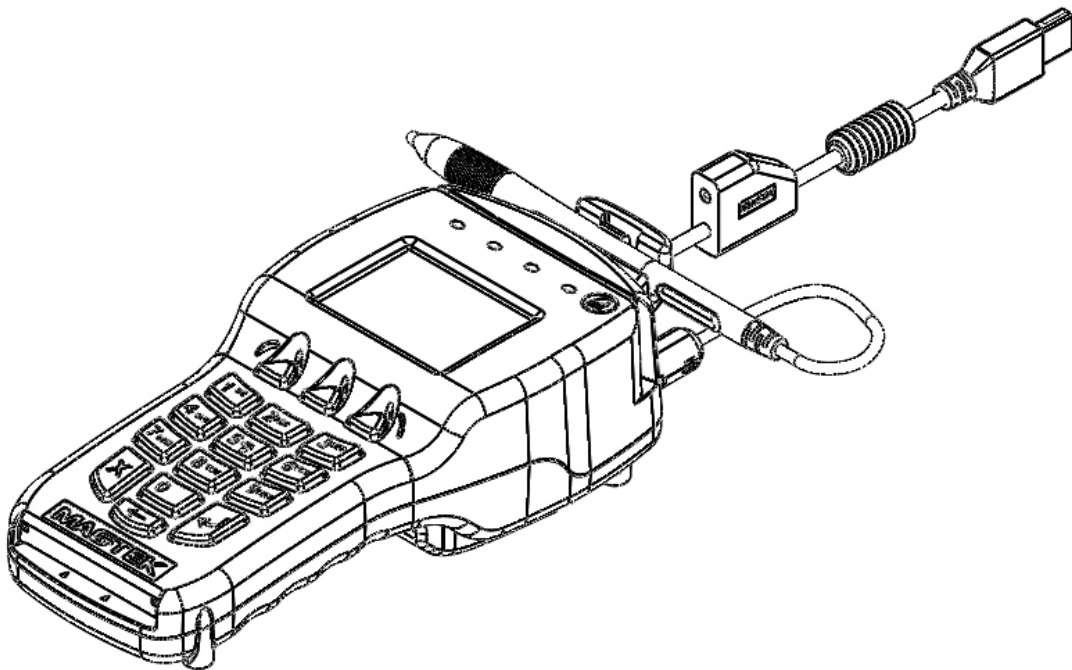


Figure 3-1. USB Interface

3.2 Ethernet Installation

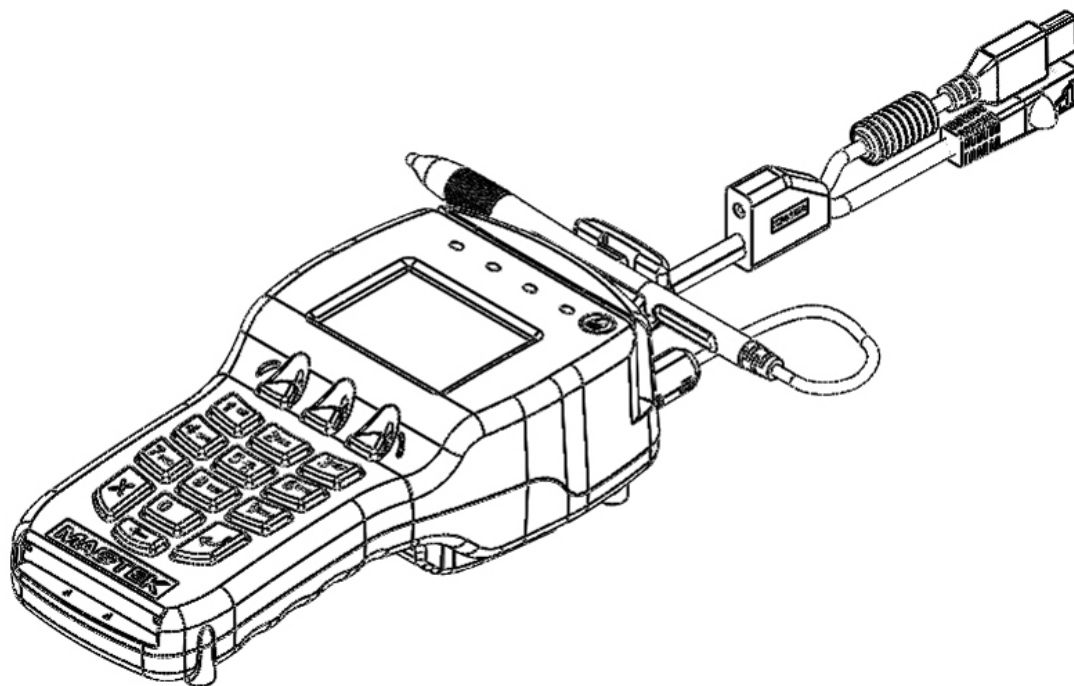


Figure 3-2. Ethernet Interface

3.3 Privacy Shield Installation

To install the Privacy Shield, follow the steps below.

Place the clips of the open end of the Privacy Shield into the openings located just above the contact card slot as shown in Figure 3-2.

Pivot the shield down, locking the three clips into the holes located just above the function buttons.

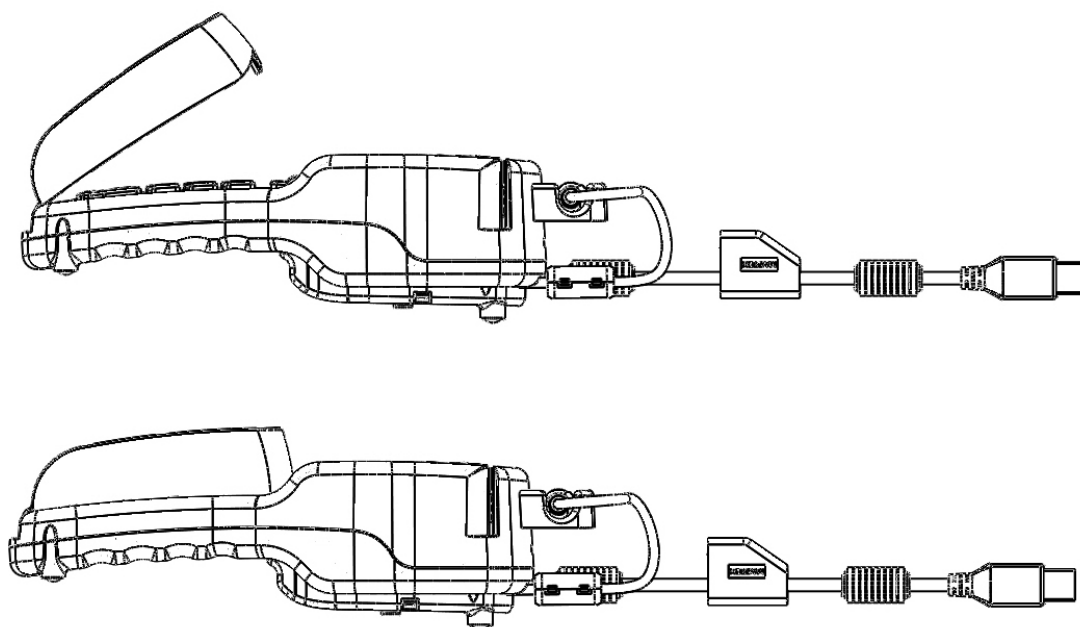


Figure 3-3. Installing the Privacy Shield

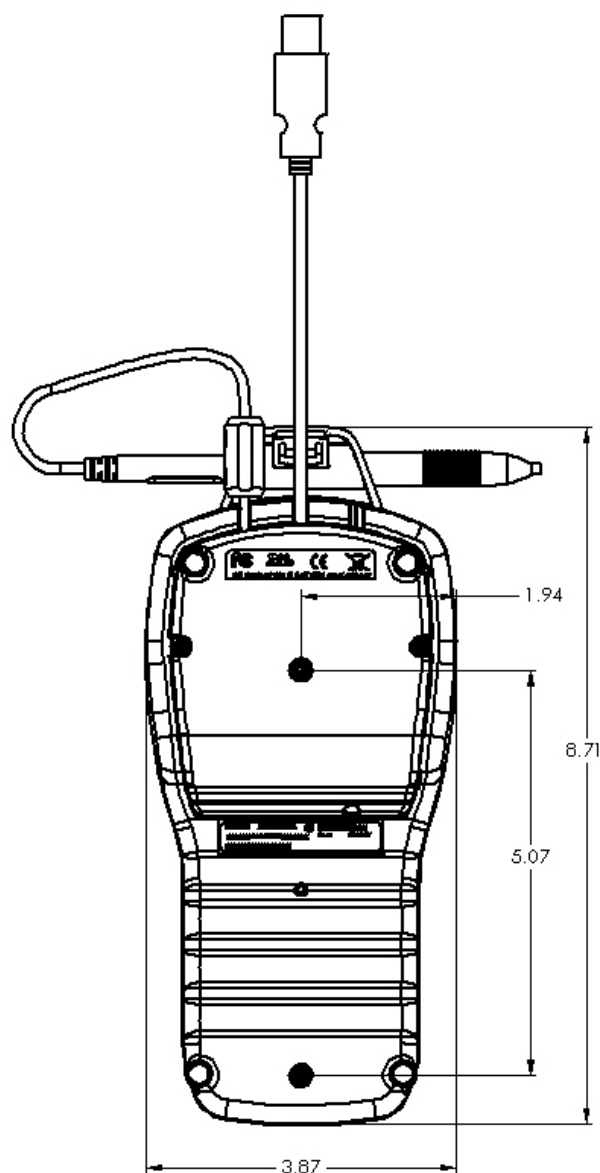
3.4 Privacy Shield Removal

To remove the Privacy Shield, follow the steps below.

Grasp the Privacy Shield and slowly lift the edge closest to the LCD, pivoting the shield up to a 45 degree angle and remove the shield.

3.5 Mounting Dimensions

The overall dimensions of the unit and the mounting hole locations are shown in Figure 3-4. This drawing is not to scale and dimensions are given in inches. In addition, mounting the DynaPro to a surface will require size # 4-40 screws.



Notes: All dimensions are XX= +/- 0.02 in inches.

Figure 3-4. Mounting Dimensions and Cable Access Hole

4 OPERATION

4.1 Overview

During normal operation, the operator will select the type of transaction from the PC application controlling the DynaPro and the cardholder will enter data on the DynaPro's keypad in response to prompts on its LCD. Transactions may include new accounts, teller window applications, checking, savings, mortgages, retail transactions, or any other option where there is interaction between the cardholder and the operator.

NOTICE

Messages shown on the DynaPro are customized by the application programmer; therefore, the sequence of prompts on the LCD and their contents will vary depending on the requirements of the institution and may not correspond to the example messages contained herein. Refer to appropriate personnel if there are any questions about the prompts or any part of the operation.

The DynaPro will display “Welcome” on its LCD (see figure 4-1 for an example) to indicate that it is ready to enter a new transaction.



Figure 4-1. Example of Welcome Screen (Ready for a New Transaction)

Typically, the cardholder is prompted to swipe his or her card through the DynaPro's MSR to initiate a transaction. If the card swipe failed to read the card data, the application may request the user to re-swipe the card or may ask the user to enter the card data manually. The application may also need to prompt the user to identify the card type (e.g. Debit or Credit). If a PIN is required (e.g. for a Banking or Debit card transaction), the application will prompt the cardholder to enter his or her PIN. If your DynaPro has signature capture capability, the application will prompt the user to enter his or her signature on the touch screen. For a more detailed discussion, see the sections below on Card Reading, Manual Card Entry, PIN Entry, and Signature Capture.

4.2 Card Reading using the SCR

When the appropriate prompt appears (see Figure 4-2 for an example), swipe the card with the magnetic stripe down and facing toward the keypad of the DynaPro as indicated in Figure 4-2 below. If the magnetic stripe data could not be read, the application may prompt the user to swipe the card again.

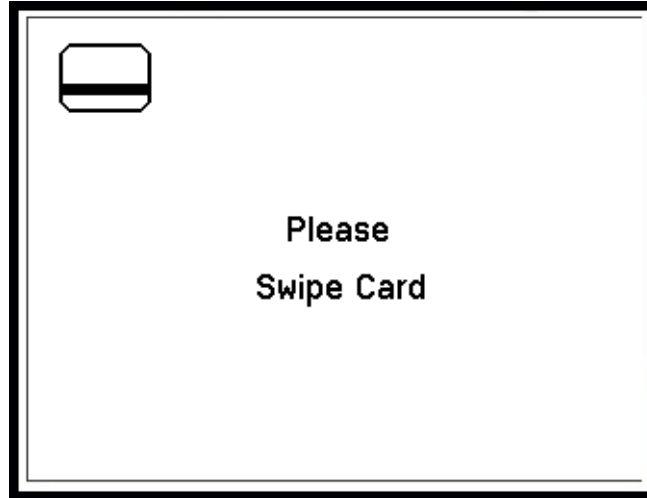


Figure 4-2. Example of Swipe Card Screen

4.3 Manual Card Entry

If the swiped card's magnetic stripe is damaged or unreadable, the application controlling the DynaPro may prompt the cardholder to enter information from his or her card manually, as shown in the following example:

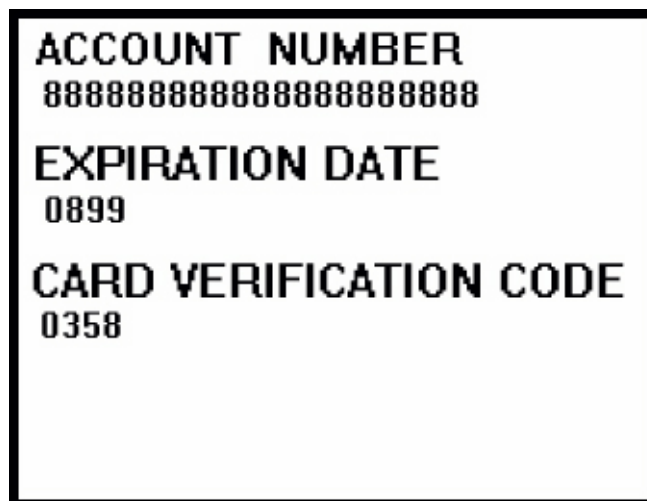


Figure 4-3. Example of User Screen to Manually Enter Card Data

The account number field can be configured with a minimum of 9 and a maximum of 19 digits, or a minimum of 14 and a maximum of 21 digits. Expiration date consists of 4 digits. The card verification code can be 3-4 digits in length.

4.4 Selecting the Card Type

In a retail setting, the transaction might require the user to select the card type (e.g. “Debit or Credit”). In the following example, the application prompts the user to press the Left function key if the card is a Credit card or to press the Right function key if the card is a Debit card:

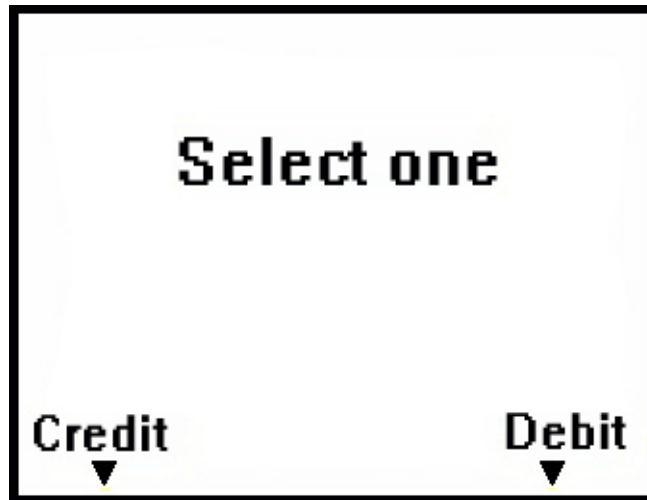


Figure 4-4. Example of User Screen to Select Card Type

4.5 PIN Entry

When PIN entry is required, the LCD will prompt the cardholder to enter his or her PIN (the PIN field has a minimum of 4 and a maximum of 12 digits for PIN entry) as required by the financial institution (see figure 4-5 for a sample LCD display). After the cardholder has entered a PIN, the ENTER key must be pressed.

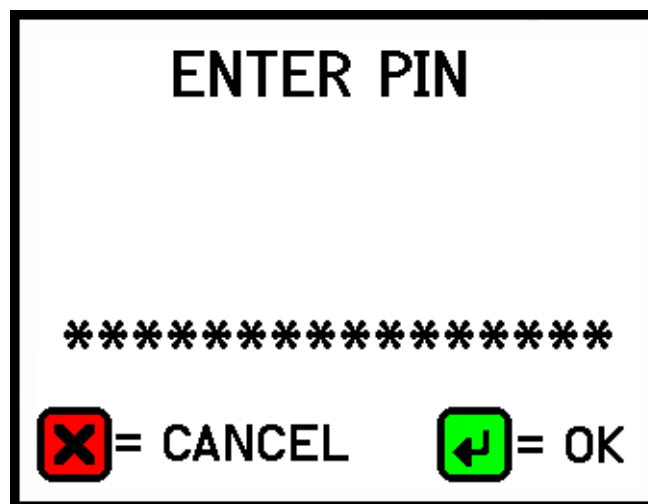


Figure 4-5. Example of User Screen to Enter PIN

If the double PIN entry option is enabled, the LCD will prompt the cardholder to reenter his or

her PIN for confirmation. The user must repeat the above process and enter the correct PIN a second time, followed by the ENTER key.

4.6 Amount Verify

In a retail setting when the customer selects “Credit” they are then prompted to verify the amount of the transaction. The customer can select “Yes” or “No” as shown in the following example:

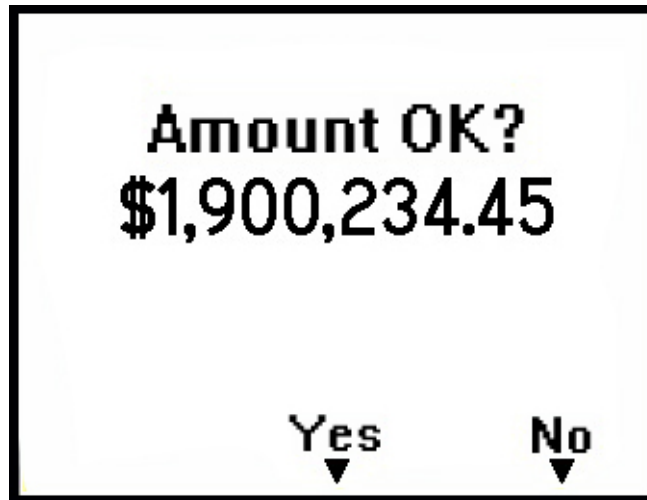


Figure 4-6. Example of User Screen to Verify Amount

4.7 Signature Capture

If your DynaPro has signature capture capability, the LCD will prompt the cardholder to enter a signature to complete the transaction (see figure 4-7 for a sample LCD display). After the cardholder has entered his or her signature, the ENTER key must be pressed.



Figure 4-7. Example of User Screen to Enter Signature

4.8 Card Reading using the Smartcard Reader for an EMV Transaction

An EMV transaction is started by the host sending an amount to be approved by a cardholder, as shown in [Amount Verify](#).

After the cardholder accepts the amount, the device will prompt the cardholder to insert his smartcard by showing:

When the appropriate prompt appears (see Figure 4-8 for an example), insert the card with the smartcard contacts facing up and the magnetic stripe facing down as indicated in Figure 4-8 below.



Figure 4-8. Example of EMV card insertion

The display will then show processing. If the Smartcard data could not be read, the application may prompt the user to insert the card again

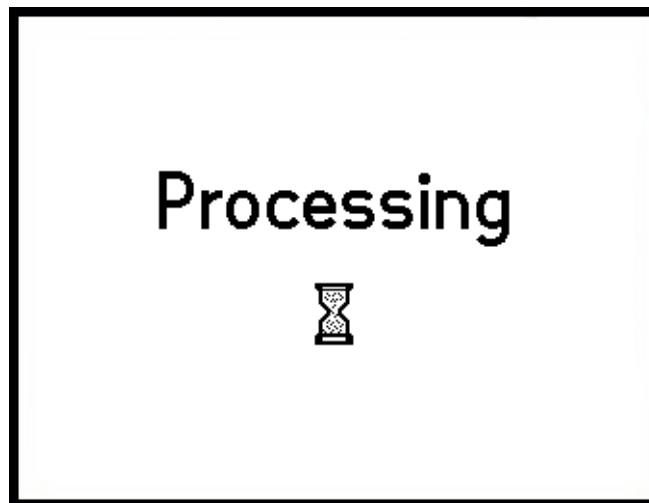


Figure 4-9. Processing Screen

Depending on the requirements of the smartcard, the device may ask for signature or PIN. If PIN entry is required, the device will ask the cardholder to enter PIN using this screen:



Figure 4-10. Example of Enter PIN Screen for EMV Transactions

Processing continues, after which the DynaPro will show the outcome – whether the transaction is APPROVED, DECLINED or TERMINATED.

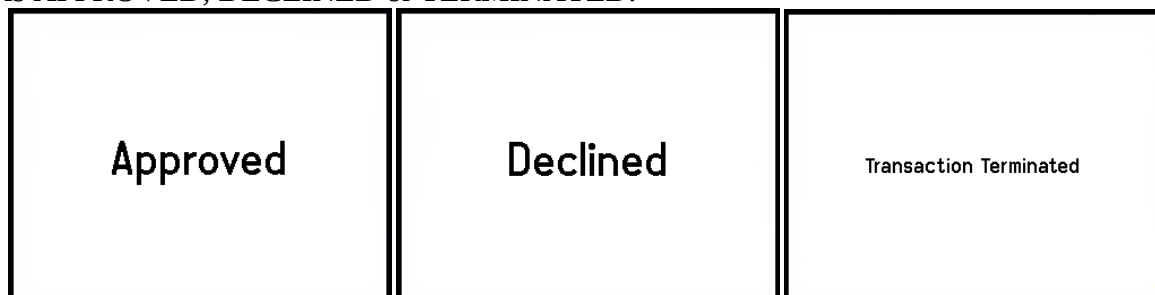


Figure 4-11. Examples of Screen Approved, Declined or Terminated

Transaction data will be sent to the host, and as the last step of the EMV transaction process, the DynaPro will ask the cardholder to remove the smartcard by displaying:



Figure 4-12. Examples of Screen Remove Card

4.9 Status Codes

The **Device Offline** screen indicates that the device is not ready for normal operation. There is also a code in the lower right corner that can help explain the cause of the **offline** state. Codes that start with H, S, C, or K indicate a problem with the unit that will require the device to be returned to the supplier for service or replacement.

Code Type	Description
A	An offline code beginning with "A" indicates the device is awaiting authentication. This is a normal condition when a unit configured to require authentication (security level 4). Authentication by the host application is required to return it to the "Welcome" screen.
C	An offline code beginning with "C" indicates the device is missing a certificate. It is recommended that the device should be repaired or replaced.
H	An offline code beginning with "H" indicates there is a hardware problem with the device. Should any H code be presented, it is recommended that the DynaPro be repaired or replaced.
K	An offline code beginning with "K" indicates a problem with either the MSR or PIN key. If it is a new device, it is likely due to the PIN Key not being loaded. A new device showing this code should be returned to the supplier for Key loading. If the code appears after being deployed and used for a long period of time, this code would be presented if one or both DUKPT keys have been exhausted. If this is the case it is recommended that you contact the supplier for a replacement.
S	An offline code beginning with "S" indicates a security element failure. This code can be triggered through severe handling of the device or strong interference by a nearby EMF source. If you move the device away from any suspected EMF source and the error continues, the device should be repaired or replaced.

5 MAINTENANCE

5.1 Cleaning

Periodic cleaning of the DynaPro's exterior may be required. To clean the outside of the DynaPro, wipe down the unit with a soft, damp cloth and then wipe with a dry cloth.

⚠ CAUTION

Avoid excessive use of liquid cleaning products and do not attempt to clean the card path with any objects other than approved cleaning cards or compressed air.

5.2 Adjusting the LCD

If it becomes necessary to adjust the LCD brightness or contrast, press the Left function key, followed by "523" (corresponding to the letters "LCD"), followed by the Right function key. The LCD will display the following screen:

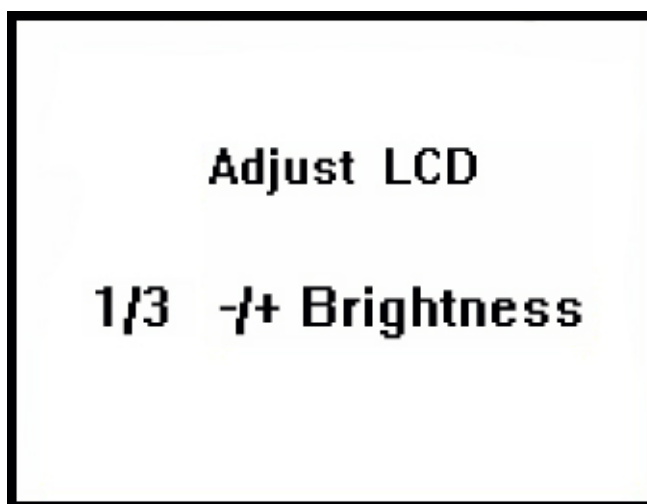


Figure 5-1. Adjusting the DynaPro's LCD

Once the above screen has displayed, press 1 to decrease, or 3 to increase, the brightness. Hit the green arrow key to accept your brightness setting.