

DynaPAD

MagneSafe Swipe Reader and Keypad Installation and Operation Manual



October 2015

Manual Part Number:
D998200104-10

REGISTERED TO ISO 9001:2008

Copyright © 2006 - 2015 MagTek, Inc.
Printed in the United States of America

Information in this publication is subject to change without notice and may contain technical inaccuracies or graphical discrepancies. Changes or improvements made to this product will be updated in the next publication release. 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.
MagnePrint® is a registered trademark of MagTek, Inc.
Magensa™ is a trademark of MagTek, Inc.
MagneSafe™ is a trademark of MagTek, Inc.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation.

All other system names and product names are the property of their respective owners.

Table 0-1 - Revisions

Rev Number	Date	Notes
10	10/30/2015	Initial Release

LIMITED WARRANTY

MagTek warrants that the products sold pursuant to this Agreement will perform in accordance with MagTek's published specifications. This warranty shall be provided only for a period of one year from the date of the shipment of the product from MagTek (the "Warranty Period"). This warranty shall apply only to the "Buyer" (the original purchaser, unless that entity resells the product as authorized by MagTek, in which event this warranty shall apply only to the first repurchaser).

During the Warranty Period, should this product fail to conform to MagTek's specifications, MagTek will, at its option, repair or replace this product at no additional charge except as set forth below. Repair parts and replacement products will be furnished on an exchange basis and will be either reconditioned or new. All replaced parts and products become the property of MagTek. This limited warranty does not include service to repair damage to the product resulting from accident, disaster, unreasonable use, misuse, abuse, negligence, or modification of the product not authorized by MagTek. MagTek reserves the right to examine the alleged defective goods to determine whether the warranty is applicable. Without limiting the generality of the foregoing, MagTek specifically disclaims any liability or warranty for goods resold in other than MagTek's original packages, and for goods modified, altered, or treated without authorization by MagTek.

Service may be obtained by delivering the product during the warranty period to MagTek (1710 Apollo Court, Seal Beach, CA 90740). If this product is delivered by mail or by an equivalent shipping carrier, the customer agrees to insure the product or assume the risk of loss or damage in transit, to prepay shipping charges to the warranty service location, and to use the original shipping container or equivalent. MagTek will return the product, prepaid, via a three (3) day shipping service. A Return Material Authorization ("RMA") number must accompany all returns. Buyers may obtain an RMA number by contacting Technical Support at (888) 624-8350.

EACH BUYER UNDERSTANDS THAT THIS MAGTEK PRODUCT IS OFFERED AS-IS. MAGTEK MAKES NO OTHER WARRANTY, EXPRESS OR IMPLIED, AND MAGTEK DISCLAIMS ANY WARRANTY OF ANY OTHER KIND, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IF THIS PRODUCT DOES NOT CONFORM TO MAGTEK'S SPECIFICATIONS, THE SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT AS PROVIDED ABOVE. MAGTEK'S LIABILITY, IF ANY, SHALL IN NO EVENT EXCEED THE TOTAL AMOUNT PAID TO MAGTEK UNDER THIS AGREEMENT. IN NO EVENT WILL MAGTEK BE LIABLE TO THE BUYER FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF, OR INABILITY TO USE, SUCH PRODUCT, EVEN IF MAGTEK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY.

LIMITATION ON LIABILITY

EXCEPT AS PROVIDED IN THE SECTIONS RELATING TO MAGTEK'S LIMITED WARRANTY, MAGTEK'S LIABILITY UNDER THIS AGREEMENT IS LIMITED TO THE CONTRACT PRICE OF THIS PRODUCT.

MAGTEK MAKES NO OTHER WARRANTIES WITH RESPECT TO THE PRODUCT, EXPRESSED OR IMPLIED, EXCEPT AS MAY BE STATED IN THIS AGREEMENT, AND MAGTEK

DISCLAIMS ANY IMPLIED WARRANTY, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

MAGTEK SHALL NOT BE LIABLE FOR CONTINGENT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES TO PERSONS OR PROPERTY. MAGTEK FURTHER LIMITS ITS LIABILITY OF ANY KIND WITH RESPECT TO THE PRODUCT, INCLUDING ANY NEGLIGENCE ON ITS PART, TO THE CONTRACT PRICE FOR THE GOODS.

MAGTEK'S SOLE LIABILITY AND BUYER'S EXCLUSIVE REMEDIES ARE STATED IN THIS SECTION AND IN THE SECTION RELATING TO MAGTEK'S LIMITED WARRANTY.

FCC WARNING STATEMENT

This equipment has been tested and was found to comply with the limits for a Class A 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 with 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 own expense.

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.

CANADIAN DOC STATEMENT

This digital apparatus does not exceed the Class A limits for radio noise from 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 la classe A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CE STANDARDS

Testing for compliance with CE requirements was performed by an independent laboratory. The unit under test was found compliant with standards established for Class A devices.

UL/CSA

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 2002/95/EC. The marking is clearly recognizable, either as written words like "Pb-free", "lead-free", or as another clear symbol ()

Table of Contents

Table of Contents	5
1 Introduction	6
1.1 About DynaPAD.....	6
1.2 About DynaPAD Components	8
1.3 About Terminology.....	9
1.4 About Solution Planning	9
1.5 About Accessories.....	9
2 Installation	10
2.1 USB Connection.....	10
2.2 Windows Plug and Play Setup	10
2.3 Location.....	10
3 Operation	11
3.1 About the Admin Menu	11
3.2 About the Status LED	12
3.3 About Swiping Cards	14
3.4 About Manual Entry of Card Data.....	14
Appendix A Specifications.....	15
A.1 Technical Specifications	15
A.2 Mechanical Dimensions.....	17
Appendix B Reference Documents	18

1 - Introduction

1 Introduction

MagTek's DynaPAD is a secure card reader authenticator (SCRA) combined with an easy-to-use keypad and a large 2 line x 16 digit liquid crystal display (LCD) allowing for either swipe card data or manual entry of card data.

1.1 About DynaPAD

Major features of DynaPAD include:

- Hardware compatible with a PC or any computer or terminal having a USB interface
- Bi-directional card reading
- Reads encoded data that meets ANSI/ISO/AAMVA standards
- Reads up to three tracks of card data
- Ergonomically designed keypad offers good tactile feel (0-9 plus **Clear**, **Enter**, **Cancel**, **Backspace** and **Admin**)
- USB Powered, no external power supply required
- 2-line by 16-digit liquid crystal display (LCD)
- Secure Red/Green/Amber status LED
- Compatible with USB specification
- Compatible with HID specification
- Can use standard Windows HID driver for communications; no third party device driver is required
- Programmable USB serial number descriptor
- Programmable USB Interrupt-In Endpoint polling interval
- Programmable Keyboard Table to support alternate languages
- Non-volatile memory for property storage
- 6' USB-A cable
- Supplies 54 byte MagnePrint™ value
- Contains a unique, non-changeable serial number which allows tracking each device
- Encrypts all track data and the MagnePrint value
- Provides clear text confirmation data including cardholder name, expiration date, and a portion of the PAN as part of the Masked Track Data
- Mutual Authentication Mode for use with Magensa.net®

In addition to reading multiple tracks of data from a card, DynaPAD also includes MagnePrint® technology. The MagnePrint data is included with the track data on each card swiped transaction. To maximize card security, DynaPAD incorporates data encryption within its head to protect the card contents and MagnePrint information. DynaPAD is compatible with any device having a host USB interface. A card is read in the swipe reader by sliding it, stripe down, through the slot in either direction.

A Status LED (Light Emitting Diode) indicator on the device cover provides the operator with continuous status of the device's operations.

The keypad is designed to allow a user to input card data including the Primary Account Number (PAN), its Expiration Date (MMYY) and an optional CVV2 (nnnn). The 2 line x 16 digit display gives the user visual feedback for information prompts and data entered into DynaPAD.

1 - Introduction

DynaPAD conforms to the USB HID (Human Interface Device) Class specification Version 1.1. This allows host applications designed for most versions of Windows to easily communicate with the device using standard Windows HID driver API calls.

DynaPAD can be configured to operate in two different modes:

- In **HID mode**, DynaPAD behaves like a vendor-defined Human Interface Device (HID) with a direct communication between the host software and the device, without interference from other HID devices.
- In **Keyboard Emulation mode** (“**KB mode**”), DynaPAD emulates a USB HID United States keyboard, or optionally any international keyboard using ALT ASCII code keypad key combinations or customizable key maps. This allows host software that was originally designed to acquire card data from user keyboard input to seamlessly acquire card data from the device.

Caution

When in Keyboard Emulation mode, if another keyboard is connected to the same host and a key is pressed on the other keyboard while DynaPAD is transmitting, the data transmitted by DynaPAD may be corrupted.

When a cardholder swipes a card through DynaPAD, the track data and MagnePrint information are TDEA (Triple Data Encryption Algorithm, aka, Triple DES) encrypted using DUKPT (Derived Unique Key Per Transaction) key management. This method of key management uses a base derivation key to encrypt a key serial number that produces an initial encryption key which is injected into the device prior to deployment. After each transaction, the encryption key is modified per the DUKPT algorithm so that each transaction uses a unique key. Thus, the data is encrypted with a different encryption key for each transaction.

When a card is not present or unreadable, DynaPAD allows the user to manually enter the card data via its keypad and display. In this scenario, the Primary Account Number (PAN), Expiration Date (MMYY) and optional CVV2 (nnnn) are TDEA (Triple Data Encryption Algorithm, aka, Triple DES) encrypted using DUKPT (Derived Unique Key Per Transaction) key management, but there will be no MagnePrint information available. The output of the manually entered card data is similar to the output of a swiped card, but the Format Code on Track 1 is represented as an “M” instead of a “B”. This method allows the user to keep sensitive card data from entering a general purpose computing device where it can be more easily compromised.

1 - Introduction

1.2 About DynaPAD Components

The major components of DynaPAD are shown in **Figure 1-1**.

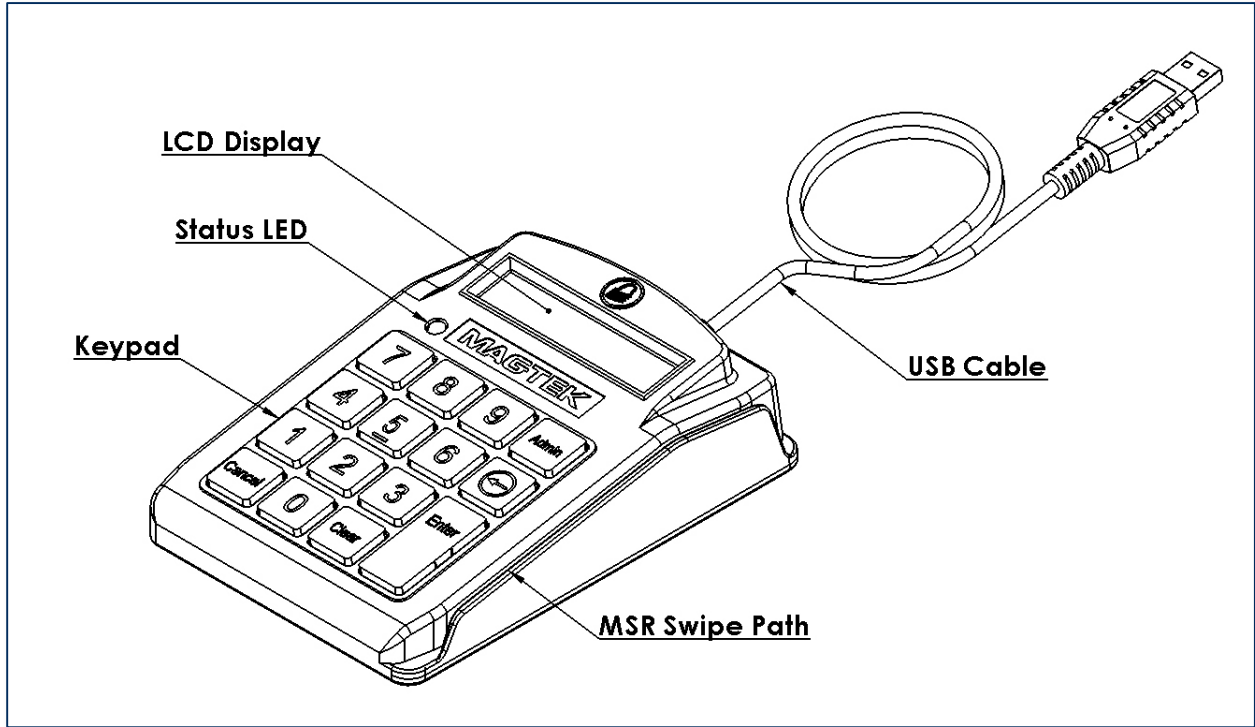


Figure 1-1 – DynaPAD Major Components

1 - Introduction

1.3 About Terminology

In this document, DynaPAD is referred to as the **device**. It is designed to be connected to a **host**, which is a piece of general-purpose electronic equipment which can send commands and data to, and receive data from, the device. Host types include PC computers/laptops, tablets, and smartphones. Generally, the host must have **software** installed that communicates with the device and is capable of processing transactions. During a transaction, the host and its software interact with the **operator**, such as a cashier or bank teller, while the device interacts with the **cardholder**.

1.4 About Solution Planning

A smooth deployment of a DynaPAD solution requires some up-front planning and decision-making:

- Determine what type of **host** DynaPAD will connect to. This will likely be a workstation with a USB port. When planning, include any additional support or devices required by the host, such as physical locations, mounting, and power connections.
- Determine what **software** will be installed on the host and how it will be configured. Software can include operating system, transaction processing software, security software, and so on. Include any additional support required by the software, such as network connections.
- Determine how DynaPAD should be **configured**, and specify that when you order devices. For example, depending on the host software's expectations, DynaPAD can present itself to the host as either a vendor-defined HID device or as a keyboard ("KB mode").
- Determine how DynaPAD will be physically **presented** to the operator. For example, consider workstation ergonomics.

1.5 About Accessories

The optional accessories are as follows:

Part Number	Description
21042806	USB MSR Demo Program with Source Code (CD)
99510026	USB MSR Demo Program with Source Code (WEB)

2 - Installation

2 Installation

This section describes the cable connection, the Windows Plug and Play Setup, and the physical mounting of the device.

2.1 USB Connection

Connect the USB cable to a USB port on the host. **Table 2-1** lists the pinouts for the DynaPAD cable.

Table 2-1 - Pinouts for DynaPAD USB Connector

Pin Number	Signal	Cable Color
1	VBUS	Red
2	- Data	White
3	+Data	Green
4	Ground	Black

2.2 Windows Plug and Play Setup

On Microsoft Windows hosts, the first time the device is plugged into a specific USB port, Windows pops up a dialog box to guide you through installing a device driver. The driver Windows installs for DynaPAD is part of the operating system and is used for all Human Interface Devices (HIDs). When the dialog box pops up, follow the on-screen instructions. After this process is completed once, Windows will no longer request this process as long as the reader is plugged into the same USB port.

2.3 Location

Choose an installation location for DynaPAD on a flat, accessible surface with at least four inches clearance on either end, to allow room to swipe a card.

3 Operation

3.1 About the Admin Menu

DynaPAD has an onboard **Admin** menu, which is accessible via the **Admin** button on the keypad. This menu allows the user to:

- Configure DynaPAD's LCD Brightness
- Configure prompts for manual input of CVV2
- Configure behavior for Primary Account Number final digit MOD10 verification.

The LCD Brightness can be set to one of three levels: Low, Medium and High.

When DynaPAD is configured to prompt for manual CVV2 entry, the device requires the cardholder or operator to input a CVV2 after the PAN and Expiration Date, before pressing the **Enter** button to complete the transaction.

When MOD10 Check is on, the device verifies the Primary Account Number as having a MOD10 check digit as the final digit of the PAN. If MOD10 Check fails, the cardholder or operator is given the opportunity to **Cancel** the transaction and start over, Edit the Primary Account Number (PAN) using the **Backspace** button, or press the **Enter** button to proceed with a failed MOD10 check digit.

After the settings have been entered, the device prompts the user to press the **Enter** button to save the settings and exit the **Admin** menu. DynaPAD retains saved settings when it is power cycled.

3 - Operation

3.2 About the Status LED

DynaPAD's **Status LED** (see **Figure 1-1**) can light red, green, or amber, and provides feedback to the operator and cardholder about the internal state of the device. **Table 3-1** summarizes how to interpret the colors and flashing patterns.

When DynaPAD is powered off, the LED is off.

When DynaPAD is powered on, the LED is solid amber until the USB host enumerates the device. When enumeration succeeds, the LED turns solid green.




Solid green indicates the reader is either awaiting Authentication (if configured to require Authentication), or armed to read a card swipe or to accept manual entry of card data (if configured to NOT require Authentication).

If DynaPAD is configured to require authentication (Security Level 4), when the host successfully authenticates, the Status LED slowly blinks green to indicate the reader is armed to read a card swipe. If the host fails to authenticate, the LED turns solid red until the host completes Authentication successfully or DynaPAD is powered down.





During a card swipe, the Status LED turns off temporarily until the swipe is completed. If there are no errors after decoding the card data, the Status LED turns green for two seconds to indicate a successful read, and remains solid green to indicate the device is ready for the next operation. If the device encounters errors decoding swiped card data, the Status LED turns red for two seconds to indicate an error occurred, then solid green to indicate it is ready for the cardholder to re-swipe. The cardholder can re-swipe indefinitely until a good read.

Anytime the host puts the reader into Suspend mode, the Status LED turns off. After the host takes the reader out of suspend mode, the Status LED returns to solid green. Authenticated mode is always ended by a USB suspend.

Table 3-1 - DynaPAD Status LED Meaning

Color	Flashing Pattern	Meaning
Off	Off 	The device is powered down or the USB host has put it into Suspend mode.
Green	Steady On 	If the device is configured to require authentication, the device is waiting for authentication. After authentication is established it slowly blink greens, or turns steady red if authentication fails. If the device is powered by USB and not configured to require authentication, the device is ready to read a card or receive keypad entries.
Green	Two Seconds On 	The device has successfully decoded a swiped card.

3 - Operation

Color	Flashing Pattern		Meaning
Green	Slow Blinking		If configured to require authentication, authentication has been established, device is ready to read a card.
Amber	Steady On		Device is powered by USB and is waiting for the host to establish a USB data connection.
Red	Steady On		If powered by USB and the device is configured to require authentication, authentication has failed. Make sure you are connecting to the correct host, and check the authentication configuration on the host.
Red	One Second On		Device has failed to decode data on a swiped card. Try the swipe again.

3 - Operation

3.3 About Swiping Cards

A card may be swiped through the reader slot when the LED is solid green or flashing green. The magnetic stripe must face down and toward the keypad, and may be swiped in either direction. If there is data encoded on the card, DynaPAD attempts to read the data, encrypt it, and send the results to the host via a USB HID input report or, if in Keyboard Emulation mode, as if the data was being typed on a keyboard. After the results are sent to the host, the device is ready to read the next card.

3.4 About Manual Entry of Card Data

When a card is not present or unreadable, DynaPAD allows the operator to manually enter the card data using the keypad and display. In this scenario, the Primary Account Number (PAN, 12-19 digits), Expiration Date (MMYY, 4 digits) and optional CVV2 (3-4 digits) are TDEA (Triple Data Encryption Algorithm, aka, Triple DES) encrypted using DUKPT (Derived Unique Key Per Transaction) key management, but there will be no MagnePrint information available. The output of the manually entered card data is similar to the output of a swiped card, but the Format Code on Track 1 is represented as an “M” instead of a “B”. This method allows the operator to keep sensitive card data from entering a general purpose computing device where it can be more easily compromised.

If card data is successfully entered, DynaPAD encrypts it and sends the results to the host via a USB HID input report or, if in Keyboard Emulation mode, as if the data was being typed on a keyboard. After the results are sent to the host, the reader is ready to read the next card.

Appendix A Specifications

A.1 Technical Specifications

Reference Standards and Certifications	
Magstripe: ISO Type B, AAMVA Encryption: TDEA (3DES)-CBC using DUKPT	
Physical Characteristics	
Dimensions (L x W x H):	L 5.90 in. x W 4.00 in. x H 1.51 in. (150 mm x 102 mm x 38 mm)
Weight:	9.3 oz. (263.7 g)
User Interface Characteristics	
Display Type:	Liquid Crystal Display (LCD)
Display Size (viewable area):	2 lines x 16 characters
Display Resolution:	N/A
Keypad:	0-9, Clear, Cancel, Backspace, Admin, Enter
Card Reader:	3 track
Acceptable Swipe Speeds:	6 to 60 ips (15.4 to 152.4 cm/s)
Electrical Characteristics	
Device Type	USB
Data Connections:	USB A, compatible with USB 1.1 and USB 2.0
Battery Capacity	N/A
Battery Charge, Standby	N/A
Battery Charge, Active	N/A
Power Input	USB powered via micro USB cable
Maximum current draw	100mA maximum
Voltage Requirement	5VDC
Battery Type:	N/A
Flash Memory:	N/A
Software Characteristics	
Tested Operating System(s):	USB: Windows 7 and newer
Environmental Tolerance	
Operating temperature:	0°C to 35°C (32°F to 95°F)
Operating relative humidity:	10% to 90% noncondensing

Appendix A - Specifications

Reference Standards and Certifications	
Storage temperature:	-20 °C to 45 °C (-4 °F to 113 °F)
Storage relative humidity:	10% to 90% noncondensing
Reliability	
Mechanical Life:	1,000,000 card swipes
Battery Shelf Life:	N/A
Battery Cycle Life:	N/A

A.2 Mechanical Dimensions

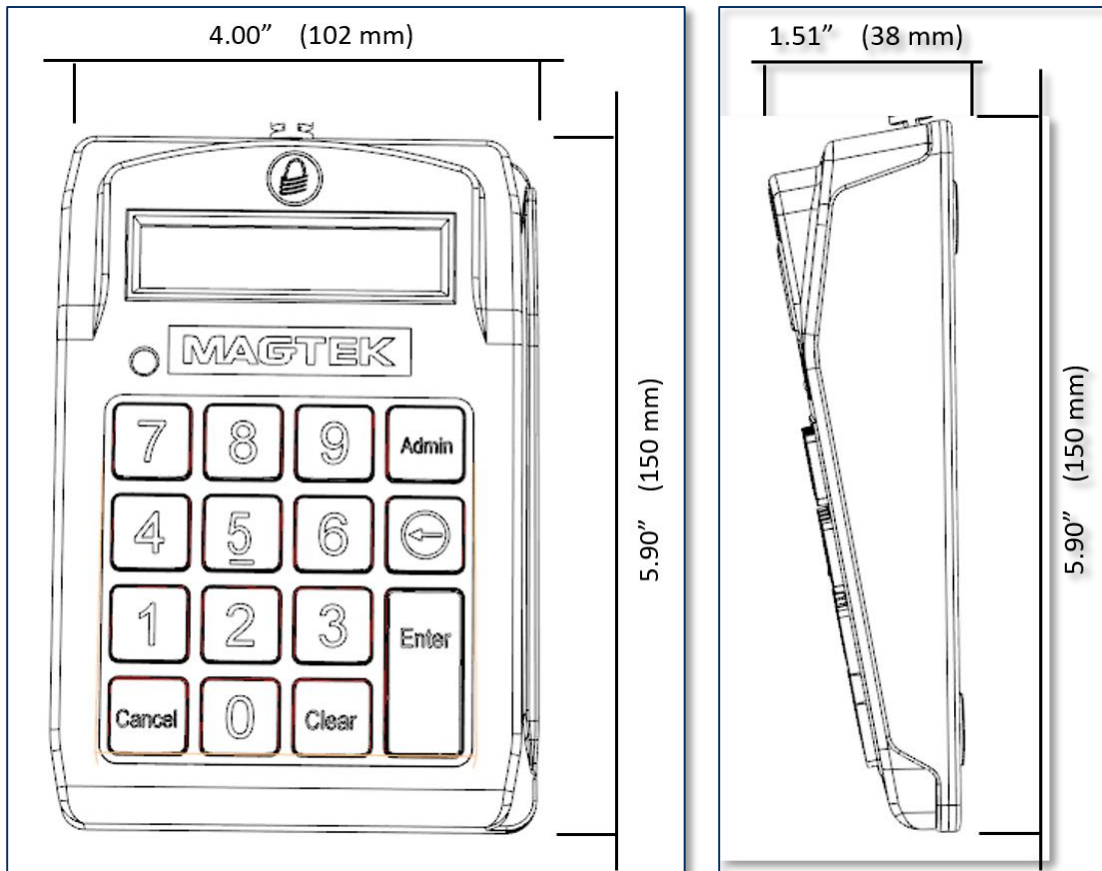


Figure 3-1 – DynaPAD Mechanical Dimensions

Appendix B Reference Documents

D99875475 MagTek Communication Reference Manual for USB MagneSafe V5 Readers

Axelson, Jan. *USB Complete, Everything You Need to Develop Custom USB Peripherals*, 1999.
Lakeview Research, 2209 Winnebago St., Madison WI 53704, 396pp., <http://www.lvr.com>

ANS X9.24-2004 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

USB Human Interface Device (HID) Class Specification Version 1.1.

Universal Serial Bus (USB): HID Usage Tables Version 1.12 (1/21/2005)

USB (Universal Serial Bus) Specification, Version 1.1, Copyright© 1998 by Compaq Computer Corporation, Intel Corporation, Microsoft Corporation, NEC Corporation.

USB Implementers Forum, Inc., www.usb.org.