DynaPAD - PN 21087008

Secure Card Reader Authenticator with Encrypting Key pad

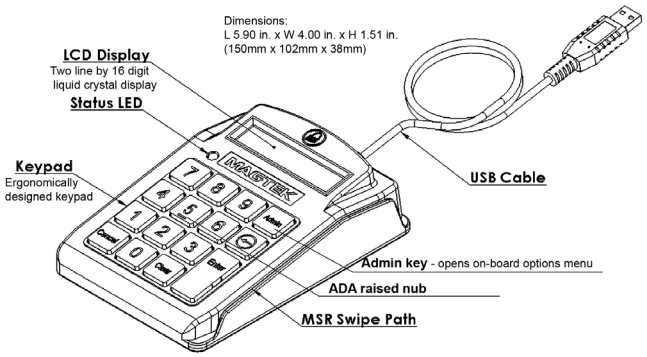
MAGTEK®
SECURITY FROM THE INSIDE

Quick Installation Guide

Setup and Installation

DynaPAD Secure Card Reader Authenticator (SCRA) is MagneSafe® secured and offers a reliable, long swipe path with complete security features for the peace of mind you can trust. DynaPAD also features an easy-to-use keypad with a large 2 line x 16 digit liquid crystal display (LCD) for manual entry of card data. Specifically designed to meet PCI DSS requirements to secure cardholder data, DynaPAD employs the industry standard, Triple DES encryption. For greater flexibility, its USB interface can be configured for USB HID or USB Keyboard Emulation, conveniently connecting to many existing merchant application and making them more secure.

Major Components



USB HID or USB KB Connection

DynaPAD can be operated in two different modes:

- HID (herein referred to as “HID mode”) and
- HID with Keyboard Emulation (herein referred to as “KB mode”)

When operating in the HID mode, DynaPAD will not use keyboard emulation. It will behave like a vendor defined HID device. When configured for the Keyboard Emulation (KB) mode, DynaPAD will emulate a USB HID United States keyboard or, optionally, any international keyboard using ALT ASCII code keypad key combinations or customizable key maps.

Windows Plug-n-Play

On hosts with the Windows operating system, the first time the reader is plugged into a specific USB port, Windows will pop up a dialog box, which will guide you through the process of installing a device driver for the reader.

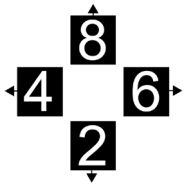
Caution: When in Keyboard Emulation mode, if another key board is connected to the same host as the reader and a key is pressed on the other keyboard while the reader is transmitting, then the data transmitted by the reader may get corrupted.

Installation Location

Installation location should be on a flat, accessible surface with at least four inches (4”) clearance on either end, to allow room to swipe a card.

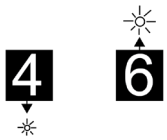
Navigating the Admin Menu

Begin by pressing the ADMIN button on the top right of the keypad. Scroll through the additional administrative options by pressing the 2 button.



Navigation

Press 4 to navigate Left.
Press 6 to navigate Right.
Press 2 to navigate Down.
Press 8 to navigate Up.



LCD Brightness

Press 2 to see the LCD Brightness setting. Options include Low, medium and High. Pressing the 4 button lowers the LCD Brightness. Pressing the 6 button increases the LCD Brightness.

CVV Setting

Press 2, after LCD brightness settings, for the CVV setting. Press 4 to turn this setting Off or press 6 to turn this setting On.

MOD10

Press 2, after CVV setting, for MOD10 Check verification setting. Press 4 to turn this setting Off or press 6 to turn this setting On. Press 2, after MOD10, for the Exit prompt, “TO EXIT AND SAVE PRESS ENTER”. Press the Enter button to save the settings and complete administrative tasks.

LED

The reader has one LED on the reader body. The LED indicator will be either off, red, green, or amber. When the reader is not powered, the LED will be off. When the reader is first plugged in, the LED will be solid amber. After the reader is plugged in, the host will try to enumerate the reader. Once the reader is enumerated the LED will turn solid green.

Use and Compliance

Card Read

A card may be swiped through the reader slot when the LED is solid green or flashing green. The magnetic stripe must face toward the keypad and may be swiped in either direction. If there is data encoded on the card, DynaPAD will attempt to read the data, encrypt it, and then 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 reader will be ready to read the next card or accept manual entry of card data for a card-not-present transaction.

Manual Card Entry

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. 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.

Technical Support

When contacting the support team please have your reader charged and have the part number and serial number(s) available.
Call 562.415.6800 or email: support@magtek.com

Compliance

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 Réglement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

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

Cet appareil numériqué de la classe A est conformé 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 ( ).