MAGTEK®
SECURITY FROM THE INSIDE

DynaFlex II PED

PIN Entry Device

PCI PTS POI v6.2 Security Policy

October 2024

Document Number:
D998200520-101

REGISTERED TO ISO 9001:2015

MagTek Inc | 1710 Apollo Court | Seal Beach, CA 90740 | Phone: (562) 546-6400 | Technical Support: (562) 415-6800
www.magtek.com

Table 0-1 - Revisions

Rev Number	Date	Notes
10	Feb 10, 2022	Initial Release
12	Nov 02, 2022	Update for PCI-6.1 Add image to Periodic Inspection. Add WLAN related content for firmware identification, available interfaces, CAPK's, and guidance. Update pictures and images to latest version. Change PCI HW ID structure.
13	Dec 16, 2022	Remove no display option. Add additional cryptographic algorithms. Update screenshots for latest firmware
14	Feb 16, 2023	Update PCI version to 6.2. Add extra info about HW ID. Add pictures of card slot and images of kiosk mounting. Update section **3.2 Installation.** Update **section 4.1 Periodic Inspection**. Add image of product installed into Kiosk environment; 4.2. Update image to show direct image of ICCR card slot
15	Mar 22, 2023	HW ID revision change (position 11). **2.3.1Hardware Identification**, update images to show correct **HW ID and Firmware Identification** and \ change PCI ID Tag revision (position 11) to 'B'.
16	Apr 26, 2023	Add AES-256 to data protection algorithms Section 5.1
17	June 6, 2023	Add a picture showing the bottom view of device with both BCR and Kiosk options. Remove some wording in the preface. Add detail on retrieving the firmware versions. Change some language describing the DynaFlex II PED device and the hardware configurations.
18	October 3, 2023	Update Main FW in **Firmware Identification**, Update Device Information Screenshots **in Device Information Page**, Update PCI Hardware Label Images in **Hardware Identification, Self-Test** updated with revised 23/24 hour reset guidance.
19	October 18, 2023	Update WLAN FW in **2.3.2 Firmware Identification,** added FW major revision description note to **2.3.2 Firmware Identification**, Update Device Information Screenshots in **2.3.3 Device Information Page.**
1A	October 26, 2023	Add previous descriptions of 17 position Main FW version and 17 position WLAN FW to **2.3.2 Firmware Identification**
1B	November 2, 2023	Update Tables **Table 2-4 - Main Firmware Version and Associated Variables Table** 2-7 **- WLAN Firmware and Associated Variables** with updated version descriptions, changed from A to AA.

Rev Number	Date	Notes
100	June 19, 2024	Update device images in Title page, in **Figure 2-1** and **Figure 4-2;** Update **Table 2-1 - PCI Hardware Identifier, Table 2-2 – Hardware Versions with Description of Associated Variables with current HW ID numbers;** Update **Table 2-4 - Main Firmware Version and Associated Variables , Table 2-5 – Boot Firmware Version and Associated Variables** with current FW versions; Change revision number to correct 3 digit numeric revision convention, from 1B to 100, Update **Figure 2-2 - Bottom views of DynaFlex II PED, DynaFlex II PED (Kiosk), DynaFlex II PED (BCR), and DynaFlex II PED (BCR & Kiosk)** and **Figure 2-3 - DynaFlex II PED Device Label Location with updated labels**.
101	October 28, 2024	Added new ID for Main FW with newer EMV Kernels to **2.3.2 Firmware Identification**

Table of Contents

1 Purpose

This document describes how to use the DynaFlex II PED device in a secure manner. This includes information about key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements.

The use of the secure card reader in any manner not described in this security policy will invalidate the PCI PTS POI v6.2 approval of the device.

2 General Description

2.1 Product Name and Appearance

The front-facing sides of the DynaFlex II PED, including the model with an optional barcode reader (BCR), are shown in **Figure 2-1** below. The Kiosk option does not alter the front appearance of the devices. The various bottom views of all devices are depicted in

Figure 2-1 - DynaFlex II PED and DynaFlex II PED (BCR).

Figure 2-2 - Bottom views of DynaFlex II PED, DynaFlex II PED (Kiosk), DynaFlex II PED (BCR), and DynaFlex II PED (BCR & Kiosk)

2.2 Product Type

The DynaFlex II PED device includes USB communications, magnetic stripe readers (MSR), contact chip card readers (ICCR), contactless card reader (CTLS), and a color display with touchscreen that provides PIN and manual account data entry as well as signature capture capabilities. DynaFlex II PED may also be purchased with an optional embedded barcode reader (BCR) or wireless WLAN communications module.

The DynaFlex II PED can be used as a desktop or handheld device. The Kiosk configuration uses a back cover intended for secure mounting, suitable for use in an unattended environment. All are approved as a PIN Entry Device (PED) device class under PCI PTS POI v6.2 requirements.

Usage in any other environment will invalidate the approval.

2.3 Identification

2.3.1 Hardware Identification

To find important product identification, look on the printed product label on the bottom face of the device as shown in **Figure 2-3 below**. The device may need to be temporarily detached from stands or surfaces to view the label.

NOTICE

Do not remove or alter this label.

Figure 2-3 - DynaFlex II PED Device Label Location

The printed label includes the following elements of device identification information, shown by the numbered callouts below in **Figure 2-4:**

1) Product name
2) PCI Hardware Identifier ("HW")

Figure 2-4 - DynaFlex II PED Device Label

The label also contains other supporting information about the device.

All DynaFlex II PED hardware configurations are listed in **Table 2-1 - PCI Hardware Identifier:**

Table 2-1 - PCI Hardware Identifier

PCI ID Tag	Configuration Description
40PCI4SU0xBx	DynaFlex II PED, USB
40PCI5SU0xBx	DynaFlex II PED, BCR, USB
40PCI4SW0xBx	DynaFlex II PED, USB/ WLAN
40PCI5SW0xBx	DynaFlex II PED, BCR, USB/ WLAN
40PCI4KU0xBx	DynaFlex II PED, Kiosk, USB
40PCI5KU0xBx	DynaFlex II PED, Kiosk, BCR, USB
40PCI4KW0xBx	DynaFlex II PED, Kiosk, USB/ WLAN
40PCI5KW0xBx	DynaFlex II PED, Kiosk, BCR, USB/ WLAN
40PCI4SU0xCx	DynaFlex II PED, USB
40PCI5SU0xCx	DynaFlex II PED, BCR, USB
40PCI4SW0xCx	DynaFlex II PED, USB/ WLAN
40PCI5SW0xCx	DynaFlex II PED, BCR, USB/ WLAN
40PCI4KU0xCx	DynaFlex II PED, Kiosk, USB
40PCI5KU0xCx	DynaFlex II PED, Kiosk, BCR, USB
40PCI4KW0xCx	DynaFlex II PED, Kiosk, USB/ WLAN
40PCI5KW0xCx	DynaFlex II PED, Kiosk, BCR, USB/ WLAN

Table 2-2 – Hardware Versions with Description of Associated Variables

Hardware Versions with Description of Associated Variables												
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
	4	0	P	C	I	4	S	U	0	x	B	x
	4	0	P	C	I	5	S	U	0	x	B	x
	4	0	P	C	I	4	S	W	0	x	B	x
	4	0	P	C	I	5	S	W	0	x	B	x
	4	0	P	C	I	4	K	U	0	x	B	x
	4	0	P	C	I	5	K	U	0	x	B	x
	4	0	P	C	I	4	K	W	0	x	B	x
PCI Hardware ID Number	4	0	P	C	I	5	K	W	0	x	B	x
	4	0	P	C	I	4	S	U	0	x	C	x
	4	0	P	C	I	5	S	U	0	x	C	x
	4	0	P	C	I	4	S	W	0	x	C	x
	4	0	P	C	I	5	S	W	0	x	C	x
	4	0	P	C	I	4	K	U	0	x	C	x
	4	0	P	C	I	5	K	U	0	x	C	x
	4	0	P	C	I	4	K	W	0	x	C	x
	4	0	P	C	I	5	K	W	0	x	C	x

Fixed Position	Variable "X" Position	Description of Fixed or Variable "X" in the Selection Position
1-2		40 = DynaFlex II PED
3-5		PCI = PCI Hardware
6		Front options 4 = Standard 5 = includes Barcode Reader
7		Back options S = Standard K = Kiosk Mounting
8		Interface Options U = USB W = USB + WLAN
9		Placeholder 0 = As certified.
	10	Cover Color: B = Black G = Gray W = White
11		Version B and C = as Certified
	12	minor fixes not adding functionality or related to security (e.g., change component value for antenna matching): 0 = as certified

2.3.2 Firmware Identification

The most recent firmware versions for DynaFlex II PED are **1000008593-A1-PCI**, for the secure bootloader (Boot FW), **1000008592-AB0-PCI** and **1000009711-AB0-PCI** for the core firmware (Main FW), and **1000007537-AA0-PCI** for the WLAN firmware (WLAN FW). The secure bootloader firmware version covers both the first stage (Boot0) permanently programmed into the device and the second stage (Boot1). Any changes to either Boot0 or Boot1 stages will result in a change to the Boot FW version that is visible to the user, reported by the device, and listed on the PCI Approved Devices website.

All device identification information, including firmware versions, exists as properties within the device. The host can retrieve these properties (***Property Subgroup 2.1.2.2.nn Core Firmware Information***) at any time using ***Command 0xD101 Get Property*** as described in ***D998200383 DynaFlex Products Programmer's Manual (COMMANDS)***.

Note: MagTek will now use a two-character major revision designation when a new revision is released. For example, DynaFlex II PIN Entry Devices will have revision designations that increase in length from older to newer, **Ax → AAx → ABx**.

Table 2-3 - Previous Main Firmware Version and Associated Variables (17 Position)

Firmware Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	1	0	0	0	0	0	8	5	9	2	-	B	x	-	P	C	I

Main FW		
Fixed Position	**Variable "x" Position**	**Description of Fixed or Variable "x" in the Selected Position**
1-10		1000008592 = DynaFlex II PED main firmware part number
12		A or B = Certified Version
	13	Minor revisions, bug fixes
15-17		PCI = PCI version of firmware

Table 2-4 - Main Firmware Version and Associated Variables

Firmware Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
	1	0	0	0	0	0	8	5	9	2	-	A	B	x	-	P	C	I
	1	0	0	0	0	0	9	7	1	1	-	A	B	x	-	P	C	I

Main FW		
Fixed Position	**Variable "x" Position**	**Description of Fixed or Variable "x" in the Selected Position**
1-10		1000008592, 1000009711 = DynaFlex II PED main firmware part number
12-13		1000008592 - AA or AB = Certified Version 1000009711 - AB = Certified Version
	14	Minor revisions, bug fixes
16-18		PCI = PCI version of firmware

Table 2-5 – Boot Firmware Version and Associated Variables

Firmware Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	1	0	0	0	0	0	8	5	9	3	-	A	x	-	P	C	I

Boot FW		
Fixed Position	**Variable "x" Position**	**Description of Fixed or Variable "x" in the Selected Position**
1-10		1000008593 = DynaFlex II PED Boot firmware part number
12		A = Certified Version
	13	Minor revisions, bug fixes
15-17		PCI = PCI version of firmware

Table 2-6 – Previous WLAN Firmware and Associated Variables (17 Position)

Firmware Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	1	0	0	0	0	0	7	5	3	7	-	A	x	-	P	C	I

WLAN FW		
Fixed Position	**Variable "x" Position**	**Description of Fixed or Variable "x" in the Selected Position**
1-10		1000007537 = DynaFlex II WLAN module firmware part number
12		A = Certified Version
	13	Minor revisions, bug fixes
15-17		PCI = PCI version of firmware

Table 2-7 - WLAN Firmware and Associated Variables

Firmware Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
	1	0	0	0	0	0	7	5	3	7	-	A	A	x	-	P	C	I

WLAN FW		
Fixed Position	**Variable "x" Position**	**Description of Fixed or Variable "x" in the Selected Position**
1-10		1000007537 = DynaFlex II WLAN module firmware part number
12-13		AA = Certified Version
	14	Minor revisions, bug fixes
16-18		PCI = PCI version of firmware

2.3.3 Device Information Page

While powering up, the display briefly shows a page of information about the device, including the installed firmware part numbers and versions and other identifying information. To determine a device's PCI certification status, compare the contents of this screen to the device's listing on www.pcisecuritystandards.org, ***Approved PTS Devices***. Note that in PCI listings, lowercase "x" is a wildcard meaning 'any single character.'

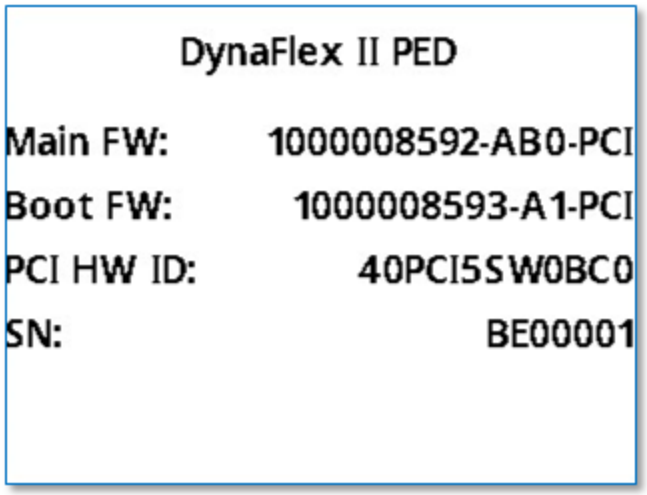

Figure 2-5 - Device Startup Screen

For WLAN device, to see details pertinent to the device's PCI certification status, including the installed firmware part numbers and versions and other identifying information (see **Figure 2-6**), on the **Welcome** screen, press the Pushbutton for 3 beeps to access to **Settings** menu, then select **Firmware**, and **Main** To return to the **Welcome** screen, select **Back** and **Exit**

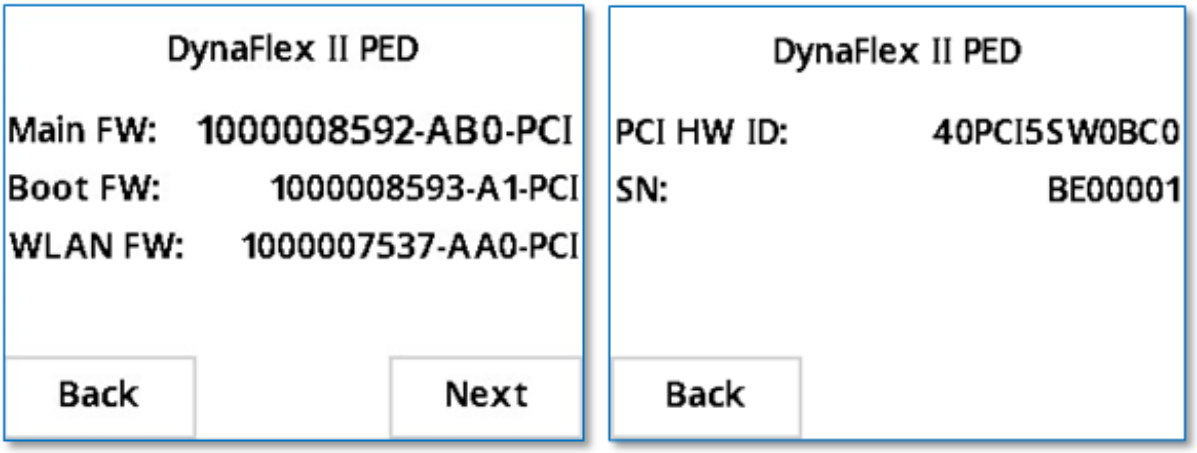

Figure 2-6 - Device Information Screen for WLAN option

3 Installation and User Guidance

3.1 Initial Inspection

After receiving the device, the customer should visually inspect the product as follows:

1) Inspect the label found on the bottom of the device (see section **2.3.1 Hardware Identification**) and make sure the label is not missing, obscured, or modified. Check the PCI Hardware Identifier on the device label and make sure it matches one of the **Hardware #** listed for the device on the PCI web site for Approved PIN Transaction Security (PTS) Devices.
2) PCI Device Validation: To check for PCI Validation check the Hardware and Firmware ID. Hardware ID is printed on the label. The Firmware ID is accessible via the device and displayed on the screen. Go to the PCI compliance web page and search for MagTek, and find the product name, DynaFlex II PED. Compare the Hardware ID and Firmware ID: https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices
3) Check the Device S/N and make sure it matches with labels on shipping materials and documentation.
4) Visually inspect the device, per ***D998200524 DYNAFLEX II PED PRODUCTS DEVICE INSPECTION*** or ***D998200539 DYNAFLEX II PED KIOSK PRODUCTS DEVICE INSPECTION*** which is included in the package with each device.
5) Follow the steps in **section 2.3.3** to view the PCI firmware versions installed on the device. Make sure this matches one of the **Firmware #** values listed on the PCI web site for DynaFlex II PED. Note that in PCI listings, lowercase "x" is a wildcard meaning 'any single character.

3.2 Installation

Connect the device to a USB host for power and control in an attended or unattended environment. The kiosk version includes features for secure mounting to a surface.

The DynaFlex II PED should be placed away from sources of heat, moisture, dust, and electromagnetic radiation (e.g., display screens, motors, and security tag mechanisms).

When mounting DynaFlex II PED with kiosk back cover, the device must be installed such that cardholders have a full, unobstructed view of the housing around the card insertion slot opening ("entry zone") and magnetic stripe reader swipe path prior to insertion or swipe see **Figure 3-1 - Unobstructed View of Card Insertion Slot and Card Swipe Path** below. This is to allow cardholders to easily detect suspicious objects in or around the card paths, such as bugs / skimmers / tapping mechanisms, wires, or antennas. Installation height is one factor in meeting this requirement. The DynaFlex II PED is designed to maximize visibility of all card paths. Assuming the solution design does not add features that obstruct the view of the slot, any practical mounting height fulfills the visibility requirement.

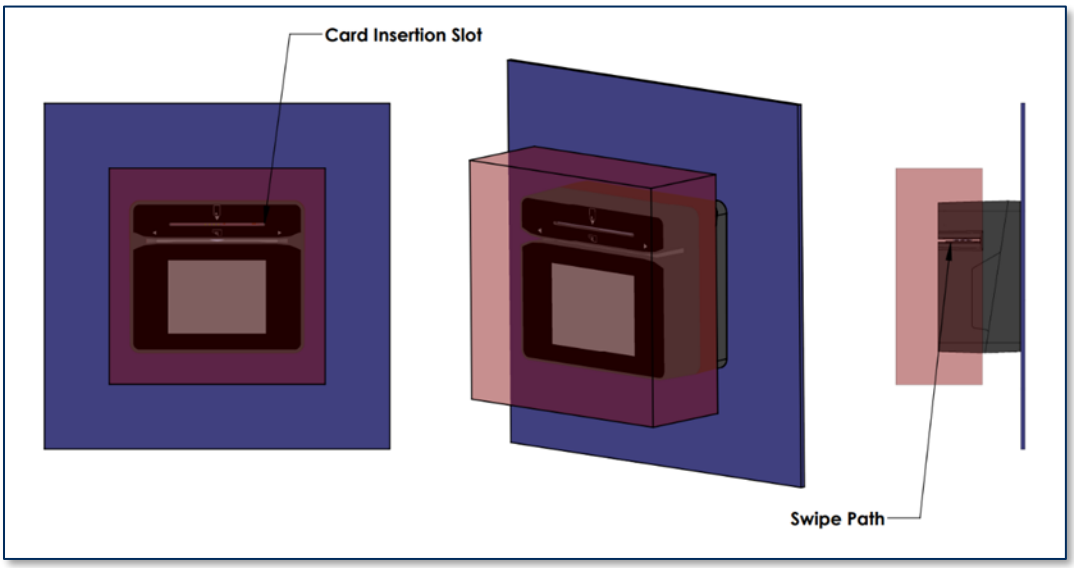

Figure 3-1 - Unobstructed View of Card Insertion Slot and Card Swipe Path

3.3 Environmental Conditions

The specified environmental conditions to operate and store the device are:

- Operating temperature range: 0°C to 45°C / 5% to 90% RH
- Storage temperature range: -10°C to 60°C / 5% to 90% RH

For safety, battery charging is disabled when the device is connected outside the recommended operating temperature range.

The security of the reader is not compromised by altering the environmental conditions outside the stated operating ranges above. Any temperature or operating voltage outside the values in the table below will trigger environmental security protections, resulting in a tamper condition. The device will need to be returned to the factory for inspection before this condition can be cleared.

Table 3-1 - Sensor Values

Sensor	Low Threshold Value	High Threshold Value
Internal Voltage	1.60V ± 0.055V	3.775V ± 0.1V
Temperature	-45°C ± 15°C	120°C ± 10°C

3.4 Communications and Security Protocols

DynaFlex II PED supports a USB interface using the USB-HID protocol and optionally 802.11 WLAN using TLS 1.2 secure WebSocket. Transactions, configuration, firmware updates, and key injection can all be performed using these interfaces. Use of any method not listed in this security policy will invalidate the device's PCI PTS approval.

3.5 Configuration Settings

DynaFlex II PED ships from the factory fully secure. The devices have no configuration settings that require modification by the user to meet PCI security requirements.

4 Operation and Maintenance

4.1 Periodic Inspection

The merchant or acquirer should daily check the appearance of secure card reader:

1) Inspect the appearance of secure card reader to make sure it is the right product.
2) Inspect whether the Swipe Path has an additional card reader or other inserted bugs, See **Figure 4-1**, below.
3) Observe the Chip Card Insertion Slot to determine whether there are any wires or obstructions. See **Figure 4-1,** below.
4) Inspect whether the product appearance has been changed.
5) Check if the firmware version is correct.
6) Observe whether there are any visual observation corridors, and deter them by body or other shields
7) Power on the secure card reader and check that the firmware runs well, as the startup will inspect the hardware security, authenticity, and integrity of firmware. Only the leftmost LED should be on and blinking green.

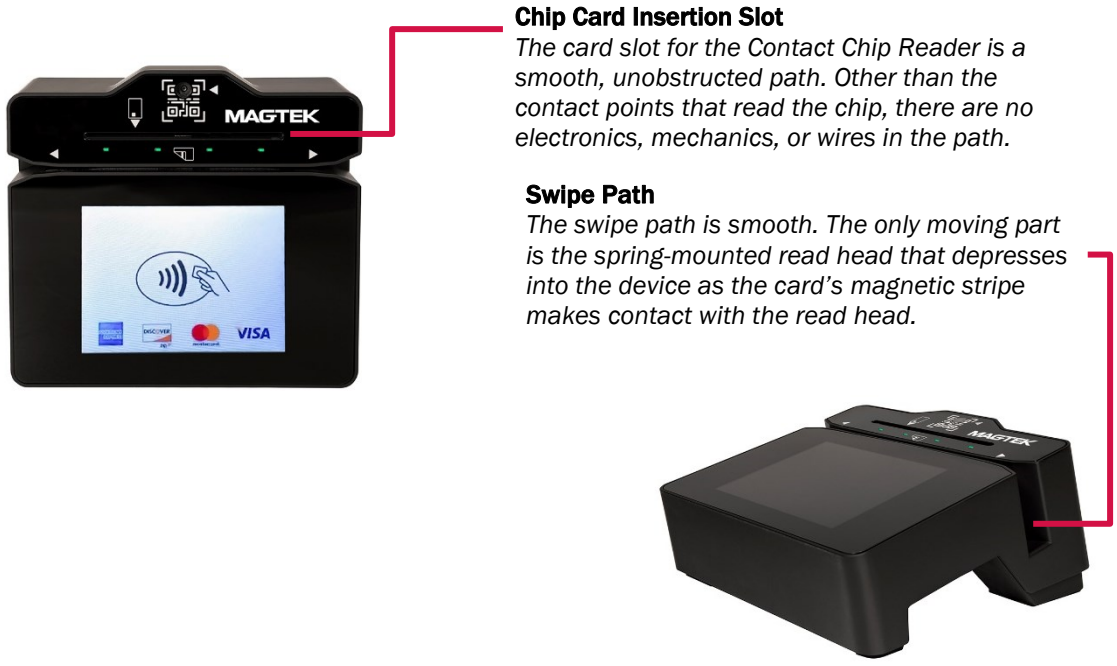

Figure 4-1 - Chip Card Insertion Slot and Swipe Path Examples

MagTek strongly recommends performing security inspections on a regular schedule. Additional information can be found in the document ***D998200524 DYNAFLEX II PED DEVICE INSPECTION***. If any problems are detected, stop using the device, set it aside in a secure location, and contact the manufacturer or your acquirer for further advice.

4.2 Self-Test

DynaFlex II PED performs self-tests at power-up and after reset. The device automatically resets and performs self-tests every 23 hours if it is configured to automatically reset 23 hours after booting, otherwise the device automatically resets and performs self-tests every 24 hours if it is configured to automatically reset at a specific time of day. No manual steps by the operator are required. Self-tests include:

- Checking the integrity and authenticity of the firmware and cryptographic keys.
- Checking security mechanisms for signs of tampering.

4.3 Roles and Responsibilities

The DynaFlex II PED has no functionality that gives access to security-sensitive services based on roles. Such services are managed through dedicated tools, using cryptographic authentication.

4.4 Passwords and Certificates

DynaFlex II PED ships from the factory fully secure. The devices have no security related default values (e.g., passwords/authentication codes/certificates) that require modification by the user to meet PCI security requirements. A custom signed trust configuration file with the customer CA certificates must be loaded by the user before TLS 1.2 protected communications can occur. The user must also configure the SSID and access point credentials to use the WLAN interface.

4.5 Tamper Response

If the device senses a physical or environmental attack, it erases all sensitive keys, and will have limited functionality. While powered on, the DynaFlex II PED indicates the tampered state has been triggered by flashing all four LEDs red (see **Figure 4-2 Tamper Response)** and displaying an "OFFLINE Tampered" prompt on the display**.**

If this occurs:

1) Remove the device from service immediately.
2) Store it securely for possible forensics investigation.
3) Contact the manufacturer for assistance. The device will likely need to be returned to the manufacturer for diagnosis and servicing.

Figure 4-2 Tamper Response

4.6 Privacy Shield

DynaFlex II PED has no privacy shield, therefore merchants must provide cardholders with the necessary privacy and guidance to enter PIN(s) safely and securely. One method is to include guidance messages and logos for the cardholder as part of a customer display driven by the host software. The figure below shows an example of a safe PIN entry logo that the host could display for the customer prior to, or in conjunction with, the PIN entry prompt message.

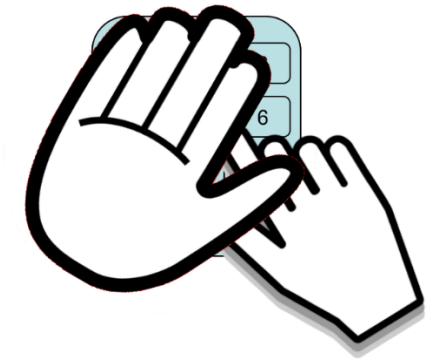

Figure 4-3 - Safe PIN Entry Logo example

Attendants should be trained to assist cardholders in ensuring that others are not looking while they are entering their PINs. The following table shows the combinations of PIN privacy methods that must be put in place when installing the device to protect the cardholder's PIN during PIN entry.

Table 4-1 - Observation Corridors

Method	Observation Corridors				
	Cashier	Customer Queue	Customer Elsewhere	On-Site Cameras	Remote Cameras
Desktop	Position device facing away from the cashier. Use signage to block cashier's view	Position device in front of the customer and the next in the queue. Customer's back to the queue	Use body to block the view of other customers	Do not install within view of cameras	Do not install within view of cameras
Mobile (handheld)	Hold the device facing away from the cashier. Use body to block cashier's view	Use body to block the view of other customers. Customer's back to the queue	Use body to block the view of other customers	Do not operate within view of cameras	Do not operate within view of cameras
Mounted	Mount device facing away from the cashier. Use signage to block cashier's view	Use body to block the view of other customers. Customer's back to the queue	Use body to block the view of other customers	Do not install within view of cameras	Do not install within view of cameras

4.7 Patching and Updating

DynaFlex II PED supports file-based updates of the device's core firmware (main firmware) and authorized commands for updating sensitive configuration. For optimal device security, MagTek recommends the latest versions of firmware should always be installed.

Firmware updates are provided as files that have been signed by MagTek. The firmware files can be loaded locally through the USB connection by using update tools available from the MagTek web site. The device verifies each update is newer than the installed version, and cryptographically authenticates the file. If version checking or authentication fails, the device erases the update file and reports an error to the host.

For help with updates to EMV configuration, contact Magensa Remote Services.

4.8 Decommissioning

Before DynaFlex II PED is permanently removed from service, all the keys and sensitive data must be erased. One way to accomplish this is by temporarily removing the bottom cover, which forces a tamper response.

If removal from service is only temporary, no action is required. All sensitive data will continue to be protected by the device's physical and logical protection mechanisms.

5 Security

5.1 Account Data Protection

The device always encrypts account data from all three reader types and manual account data entry using the 112-bit TDEA-CBC, 128-bit AES-CBC, or 256-bit AES-CBC algorithms with X9.24 DUKPT key management. This device does not support any mechanisms such as whitelists or SRED disable that would allow the data to be sent out unencrypted.

5.2 Algorithms Supported

The device uses the following cryptographic algorithms:

- AES
- TDEA
- RSA
- ECDSA (P256 and P521 curves)
- SHA-256

5.3 Communications

Wireless LAN communications use TLS 1.2 for protection. Older versions of TLS and SSL are not supported. Wireless connections to access points require WPA2. Both personal and enterprise modes (user id and password) are supported.

5.4 Key Management

The device implements AES/TDEA DUKPT as its only key management method. Use of any other method will invalidate PCI approval. DUKPT derives a new unique key for every transaction. For more details, see ***ANS X9.24 Part 3:2017***.

Table 5-1 - DynaFlex II PED Keys

Key Name	Size	Algorithm	Purpose
Transport Keys	32 bytes	AES X9.143 KBPKs	Key Injection
Account Data Key	16 bytes for TDEA and AES-128 32 bytes for AES-256	AES and TDEA DUKPT (ANS X9.24-3)	Encrypt and MAC Account Data
PIN Encryption Key	16 bytes for TDEA and AES-128 32 bytes for AES-256	AES and TDEA DUKPT (ANS X9.24-3)	Encrypt PIN
Firmware Protection Key	64 bytes for ECDSA Curve P-256	ECDSA and SHA-256	Checks integrity and authenticity of firmware
EMV CA Public keys	Varies per issuer	RSA	Authenticate card data and keys

5.5 Key Loading

The device does not support manual cryptographic key entry. Only specialized tools, compliant with key management requirements and cryptographic methods, specifically **ANSI X9.143,** can be used for key loading. Use of any other methods will invalidate PCI approval.

5.6 Key Replacement

Keys should be replaced with new keys whenever the original key is known or suspected to have been compromised, and whenever the time deemed feasible to determine the key by exhaustive attack has elapsed, as defined in ***NIST SP 800-57-1***.

6 Acronyms

Table 6-1 - Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
BCR	Barcode Reader
CTLS	Contactless
DES	Data Encryption Standard
DUKPT	Derived Unique Key Per Transaction
ECC	Elliptic-Curve Cryptography
ICCR	Integrated Circuit Card Reader
MAC	In cryptography: Message Authentication Code In networking: Media Access Control [address]
MSR	Magnetic Stripe Reader
NFC	Near Field Communication
PED	PIN Entry Device
PIN	Personal Identification Number
POI	Point Of Interaction
S/N	Serial Number
SCRA	Secure Card Reader Authenticator
SHA	Secure Hash Algorithm
SRED	Secure Reading and Exchange of Data
TDEA	Triple Data Encryption Algorithm
USB	Universal Serial Bus
USB HID	USB Human Interface Device

Appendix A References

The following documents may be used to provide additional details about the device and this security policy:

- ***D998200554 DynaFlex II Product Family Device Installation and Operation Manual***
- ***D998200383 DynaFlex Products Programmer's Manual (COMMANDS)***
- ***D998200524 DynaFlex II PED Products, Device Inspection***
- ***D998200539 DynaFlex II PED Kiosk Products, Device Inspection***
- ***D998200564 DynaFlex II Family Package Inspection***
- ***NIST SP 800-57-1 Recommendation for Key Management***
- ***ANSI X9.24 Part 3:2017, Retail Financial Services Symmetric Key Management, Part 3: Derived Unique Key Per Transaction Using Symmetric Techniques***
- ***ANSI X9.143-2022, Interoperable Secure Key Exchange Key Block Specification***