MAGTEK®
SECURITY FROM THE INSIDE

DynaFlex / DynaFlex Pro, DynaFlex Kiosk / DynaFlex Pro Kiosk

Secure Card Reader
PCI POI Security Policy

May 2021

Document Number:
D998200342-20

REGISTERED TO ISO 9001:2015

MagTek I 1710 Apollo Court I Seal Beach, CA 90740 I Phone: (562) 546-6400 I Technical Support: (888) 624-8350
www.magtek.com

Table 0-1 - Revisions

Rev Number	Date	Notes
10	Sep 25, 2020	Initial Release
20	May 21, 2021	Update product images and product names on cover page; Section **1** and throughout, clarify model groupings; Throughout, add references to kiosk models device inspection guide; **2.2** and **3.2** add unattended use of kiosk models; **Figure 2-1** update to reflect latest appearance and match order of models with introductory text; **Figure 2-2** update to show kiosk models label location and non-kiosk model change to label size; **Figure 2-3** update to reduce length, remove callout for serial number; **Table 2-1** add kiosk model hardware IDs; **3.2** add information about mounting height for kiosk models; Misc. clarifications and corrections.

Table of Contents

1 Purpose

This document addresses the proper use of DynaFlex family of SCR devices 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 method not described in this security policy, will invalidate the PCI PTS v5.1 approval of the device.

Throughout this document:

- **DynaFlex products** refers to all products in the DynaFlex product family, including DynaFlex models, DynaFlex Pro models, DynaFlex Kiosk models, and DynaFlex Pro Kiosk models.
- **DynaFlex models** refers to DynaFlex products with no display, including DynaFlex and DynaFlex Kiosk models.
- **DynaFlex Pro models** refers to DynaFlex products with a display, including DynaFlex Pro and DynaFlex Pro Kiosk models.
- **DynaFlex Kiosk models** refers to products with or without a display that are designed for installation in kiosks, including DynaFlex Kiosk and DynaFlex Pro Kiosk.

2 General Description

2.1 Product Name and Appearance

DynaFlex models (without display), **DynaFlex Pro models** (with display), and DynaFlex Kiosk models are pictured in **Figure 2-1 below**.

Figure 2-1 - DynaFlex Models Top View, DynaFlex Pro Models Top View, DynaFlex Models and DynaFlex Pro Models Bottom View, DynaFlex Kiosk Models Bottom View

2.2 Product Type

All DynaFlex products include USB communications, magnetic stripe reader (MSR), contact chip card reader (ICCR), and a contactless card reader (CTLS). DynaFlex Pro models also include a color display and touchscreen with signature capture capability.

DynaFlex non-kiosk models can be used as desktop or handheld devices. They are approved as a secure card reader (SCR) under PCI PTS 5.1 requirements for use in attended or semi-attended environments as defined below.

- Card or Proximity Payment Device is present.
- Cardholder is present.
- Cardholder completes the Transaction or, if required, an individual representing the Merchant or Acquirer assists the Cardholder to complete the Transaction

DynaFlex kiosk models can be used as desktop, handheld, or mounted devices. They are approved as a secure card reader (SCR) under PCI PTS 5.1 requirements for use in attended, semi-attended, or unattended environments as defined below.

- Card or Proximity Payment Device is present.
- Cardholder is present.
- Cardholder completes the Transaction or, if required, an individual representing the Merchant or Acquirer assists the Cardholder to complete the Transaction

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 2-2 below**.

NOTICE
Do not remove, alter, or cover this label.

Figure 2-2 - DynaFlex Products Device Label Location

The printed label includes the following elements of device identification information, shown by the numbered callouts in **Figure 2-3**:

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

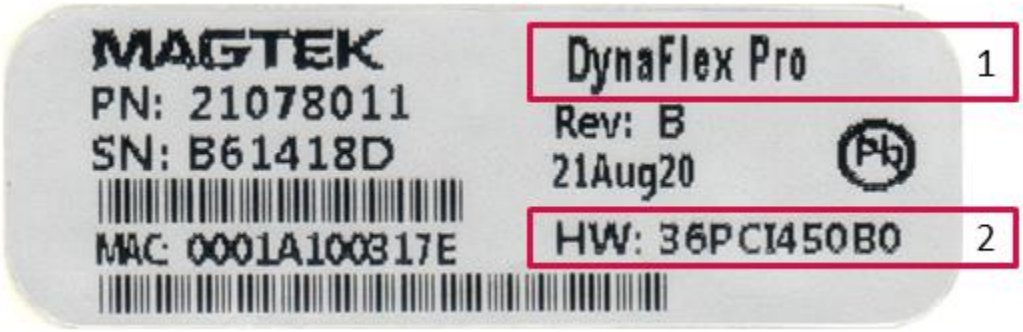

Figure 2-3 -DynaFlex / DynaFlex Pro Device Labels

The label also contains other supporting information about the device.

All of the product family's hardware configurations are listed in **Table 2-1 below**. Some configurations include hardware for additional interfaces but all interfaces other than USB are disabled in firmware. Use of any interface other than USB will invalidate PCI approval.

Table 2-1 - PCI Hardware Identifier

HW ID	Description
36PCI21xAx 36PCI21xBx	DynaFlex, No Display, USB
36PCI23xAx 36PCI23xBx	DynaFlex, No Display, USB / Bluetooth LE
36PCI41xAx 36PCI41xBx	DynaFlex Pro, Touchscreen Display, USB
36PCI43xAx 36PCI43xBx	DynaFlex Pro, Touchscreen Display, USB / Bluetooth LE
36PCI45xAx 36PCI45xBx	DynaFlex Pro, Touchscreen Display, USB / WLAN
36PCI21xBx-K	DynaFlex Kiosk, No Display, USB
36PCI23xBx-K	DynaFlex Kiosk, No Display, USB / Bluetooth LE
36PCI41xBx-K	DynaFlex Pro Kiosk, Touchscreen Display, USB
36PCI43xBx-K	DynaFlex Pro Kiosk, Touchscreen Display, USB / Bluetooth LE
36PCI45xBx-K	DynaFlex Pro Kiosk, Touchscreen Display, USB / WLAN

The lowercase x shown above in the HW ID column represent minor variations unrelated to security. The 8th character position represents color of the device, and the 10th character position represents minor non-security related changes.

2.3.2 Firmware Identification

The firmware versions for DynaFlex products are **1000007536-Ax-PCI** for the secure bootloader (Boot1 FW) and **1000007183-Ax-PCI** for the core firmware (Main FW). The lowercase x in both versions indicate minor non-security related changes. The secure bootloader firmware version also covers the initial bootloader (Boot0) permanently programmed into the device. Any changes to either Boot0 or Boot1 will result in a change to the Boot1 FW version #, visible to the user, reported by the device and listed on the PCI Approved Devices website.

All device identification information including firmware exist as properties within the device. The host can retrieve these properties at any time using ***Command 0xD101 Get Property*** as described in the ***D998200383 DynaFlex and DynaFlex Pro Programmer's Manual (COMMANDS)***.

Additionally, DynaFlex Pro models show a startup page that includes the firmware versions installed on the device. This page displays upon startup for three seconds. See **Figure 2-4**.

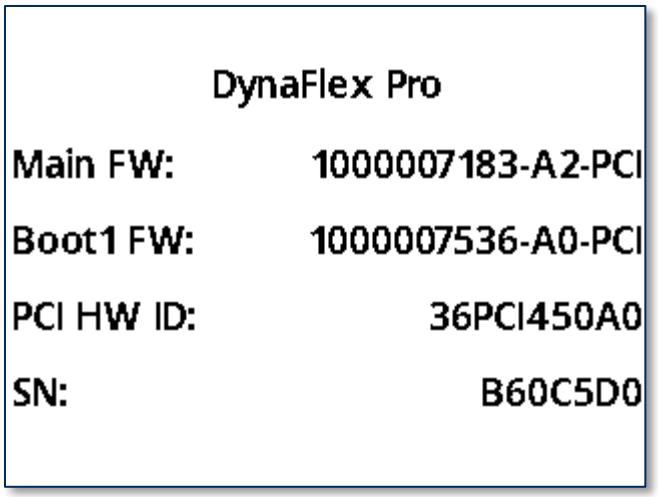

Figure 2-4 - DynaFlex Pro Models Startup Screen

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.
2) 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.
3) Check the Device S/N and make sure it matches with labels on shipping materials and documentation.
4) Visually inspect the device, per ***D998200359 DYNAFLEX DEVICE INSPECTION*** or ***D998200460 DYNAFLEX PRO KIOSK AND DYNAFLEX KIOSK DEVICE INSPECTION***, which are included in the package with each device.
5) Power on the device and make sure only the left LED is on and blinking green, indicating the device is fully functional.
6) Follow the steps in section **2.3.2** 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, DynaFlex Pro, DynaFlex Kiosk, or DynaFlex Pro Kiosk. 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 environment (or, for DynaFlex Kiosk models, an attended or unattended environment).

The SCR 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 Kiosk models, 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. This is to allow cardholders to easily detect suspicious objects in or around the card paths, such as bugs / skimmers / tapping mechanisms, and their wires or antennas. Installation height is one factor in meeting this requirement. DynaFlex products are 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.

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.

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 products support a USB interface using the USB-HID protocol. Transactions, configuration, firmware updates, and key injection can all be performed using this interface. Use of any method not listed in this security policy will invalidate the device's PCI PTS approval.

3.5 Configuration Settings

DynaFlex products ship 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 MSR card slot has an additional card reader or other inserted bugs
3) Observe the slot of smart card reader, whether there are any wires or obstructions.
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.

MagTek strongly recommends performing security inspections on a regular schedule. Additional information can be found in ***D998200359 DYNAFLEX DEVICE INSPECTION*** and ***D998200460 DYNAFLEX PRO KIOSK AND DYNAFLEX KIOSK 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

The SCR performs self-tests at power-up and after reset. The device automatically resets and performs self-tests every 23 hours. 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 secure card reader 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 products ship 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.

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 SCR indicates it is in this tampered state by blinking the leftmost LED green and setting the rightmost 3 LED's to red. 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.

4.6 Patching and Updating

DynaFlex products support 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.

4.7 Decommissioning

Before DynaFlex products are 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 using the 112 bit TDEA-CBC algorithm and 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 includes the following cryptographic algorithms:

- AES
- TDEA
- ECC-DSA (P256 curve)
- SHA-256

5.3 Key Management

The device implements original 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 Products Keys

Key Name	Size	Algorithm	Purpose
Transport Keys	32 bytes	AES TR-31 KBPKs	Key Injection
Account Data Key	16 bytes	TDEA DUKPT (ANS X9.24-3)	Encrypt and MAC Account Data
Firmware Protection Key	256 bytes	ECC-DSA SHA-256	Checks integrity and authenticity of firmware

5.4 Key Loading

The device does not support manual cryptographic key entry. Only specialized tools, compliant with key management requirements and cryptographic methods, specifically TR-31 can be used for key loading. Use of any other methods will invalidate PCI approval.

5.5 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

Acronym	Definition
AES	Advanced Encryption Standard
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:

- ***D998200382 DynaFlex Installation and Operation Manual***
- ***D998200383 DynaFlex Products Programmer's Manual (COMMANDS)***
- ***D998200359 DynaFlex Device Inspection***
- ***D998200460 DynaFlex Pro Kiosk and DynaFlex Kiosk Device Inspection***
- ***D998200361 DynaFlex Package Inspection***
- ***D998200428 DynaFlex Quick Installation Guide***
- ***NIST SP 800-57-1 Recommendation for Key Management***
- ***ANS X9.24 Part 3:2017, Retail Financial Services Symmetric Key Management, Part 3: Derived Unique Key Per Transaction Using Symmetric Techniques***
- ***X9 TR-31:2010, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms***