DynaFlex / DynaFlex Pro, DynaFlex Kiosk / DynaFlex Pro Kiosk

Secure Card Reader

PCI PTS POI v5.1 Security Policy

April 2024

Document Number:
D998200342-410

REGISTERED TO ISO 9001:2015

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; update to reflect latest appearance and match order of models with introductory text; **Figure 2-9** update to show kiosk models label location and non-kiosk model change to label size; **Figure 2-10** update to reduce length, remove callout for serial number; **2.3.1** add kiosk model hardware IDs; **3.2** add information about mounting height for kiosk models; Misc. clarifications and corrections.
30	Aug 31, 2021	Updates to correspond with firmware revision B0: **2.2** and **5.1** mention manual account entry capability; **2.3.2** update firmware version information; **3.1** remove mention of specific LED behavior (all necessary inspection steps are in the device inspection guide); **4.5** change description of LED behavior in tamper state; **2.3.1** add certified version C hardware IDs
40	Oct 28, 2021	**2.1** add images for DynaFlex models with barcode reader; **2.3.1** add barcode reader hardware IDs; **2.3.2** update latest firmware version.
41	Jan 5, 2022	Updated DynaFlex BCR image, with correct product label, in **2.3.1**.
42	Jan 3, 2024	Updated **2.3.1** to include new hardware ID Add 24 hour reset content to **4.2 Self-Test,** Update **2.3.2** with updated Firmware, Hardware ID, and Serial Numbers.
400	Feb 20,2024	Complete rewrite and update to sections**: 2.1 2.2, 2.3, 3.2, 4.1, 4.2**, **4.5**; Updated section **5** to include support for AES/DUKPT.
410	April 9,2024	Update **Table 2-2 – Hardware Versions with Description of Associated Variables** with updated fixed position values for position 11-13**, Table 2-3 - Main Firmware Version and Associated Variables** with updated description for position 12-13 as CA=Certified **, Table 2-4 – Legacy Main Firmware and Associated Variables (17 Position)** removed CC as Certified**.**

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 POI 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

The front view and back view of all **DynaFlex models** (without display), **DynaFlex Pro models** (with display, and **DynaFlex Kiosk models** are shown in **Figure 2-1** through **Figure 2-8**.

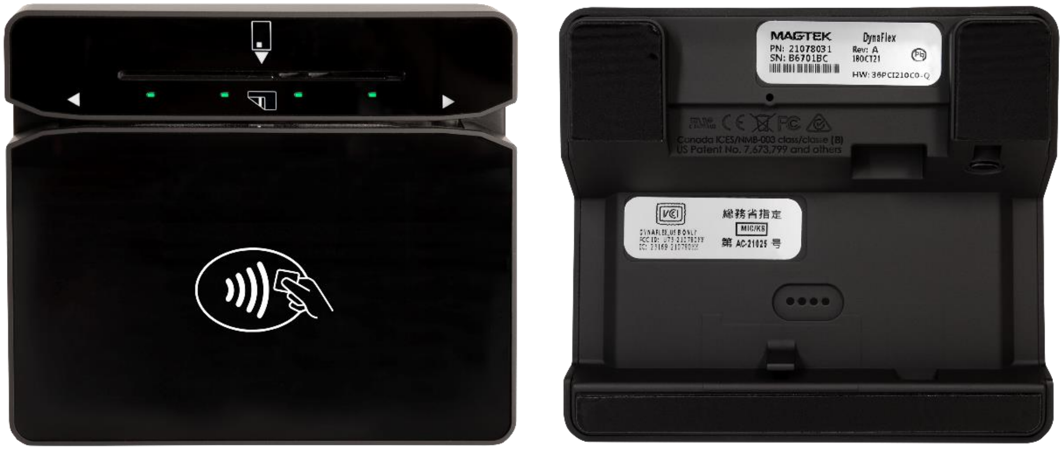


Figure 2-1 - DynaFlex Front and Back View

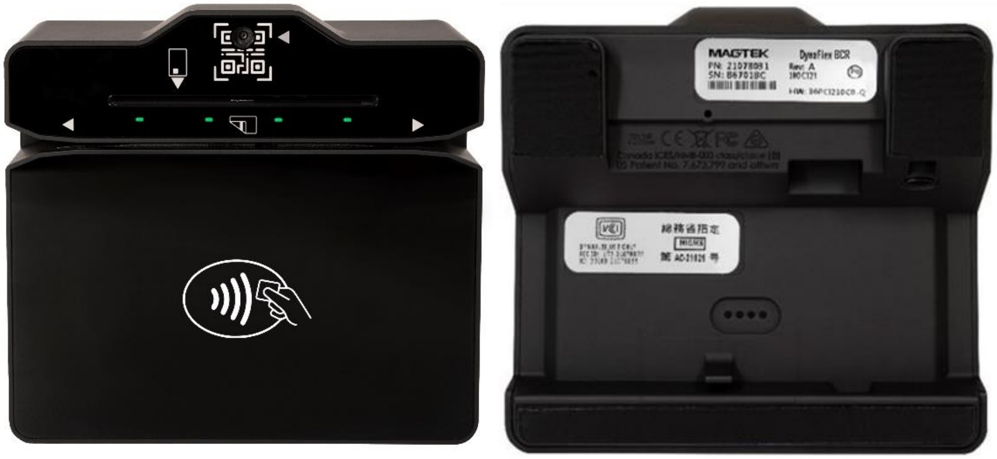


Figure 2-2 - DynaFlex with Barcode Reader Front and Back View

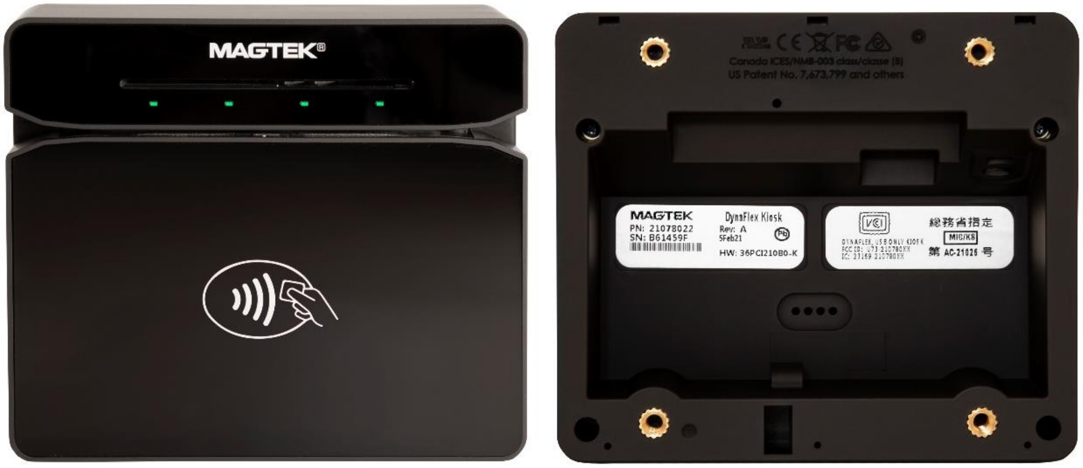


Figure 2-3 - DynaFlex Kiosk Front and Back View

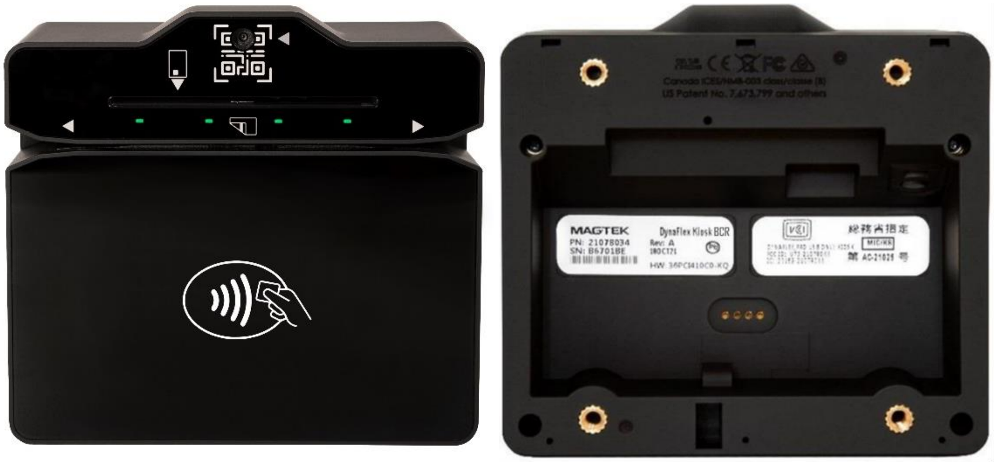

MAGTEK
DynaFlex Kiosk BCR
PN: 21078034
SN: B6701BE
Rev: A
Canada ICES/NMB-003 class/classe (B)
US Patent No. 7,673,799 and others

Figure 2-4 - DynaFlex Kiosk with Barcode Reader Front and Back View

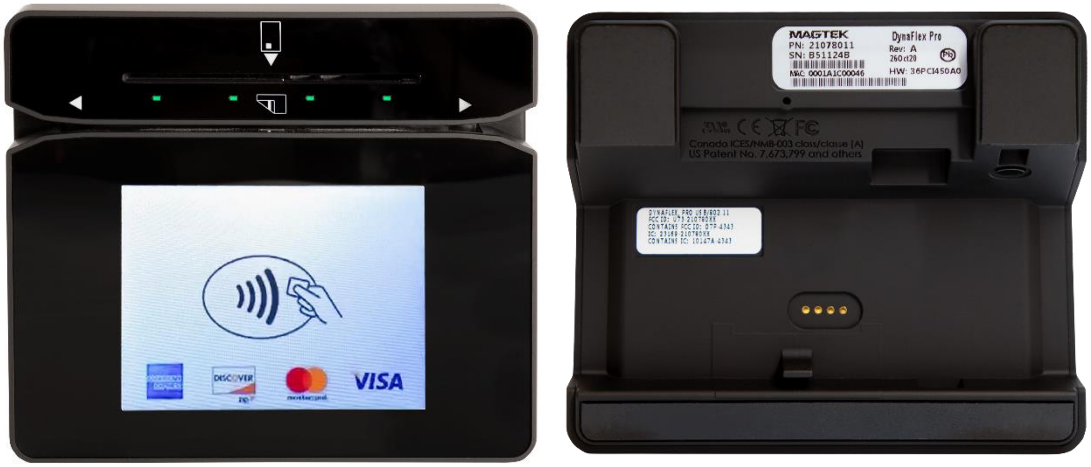

MAGTEK
DynaFlex Pro
PN: 21078011
SN: B51124B
Rev: A
HW: 36PCI450A0
Canada ICES/NMB-003 class/classe (A)
US Patent No. 7,673,799 and others
VISA

Figure 2-5 - DynaFlex Pro Front and Back View

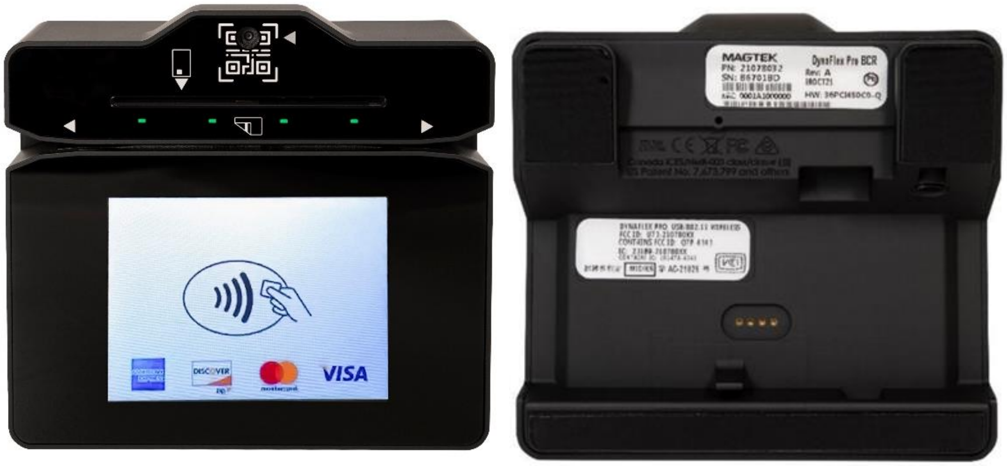


Figure 2-6 - DynaFlex Pro with Barcode Reader Front and Back View

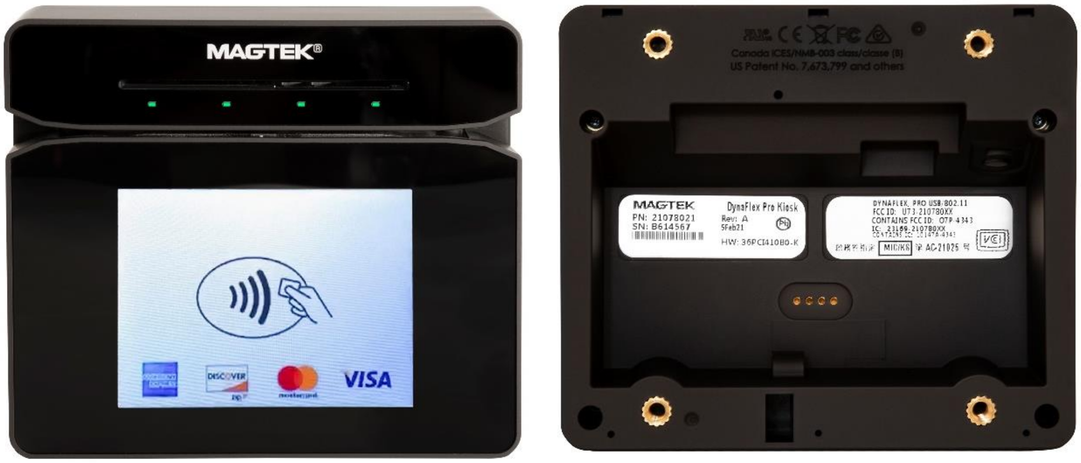


Figure 2-7 - DynaFlex Pro Kisok Front and Back View

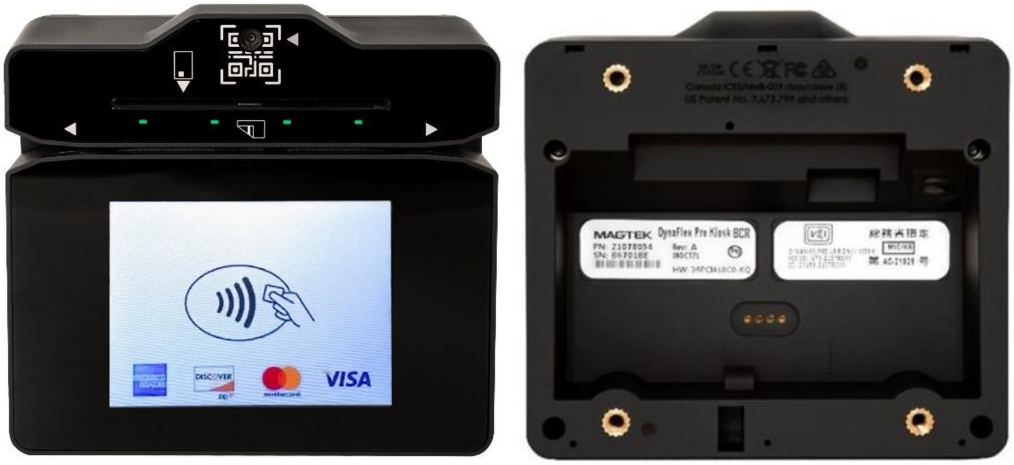


Figure 2-8 – DynaFlex Pro Kiosk With Barcode Reader Front and Back View

2.2 Product Type

DynaFlex models include USB communications, magnetic stripe readers (MSR), contact chip card readers (ICCR), and contactless card readers (CTLS). DynaFlex Pro models also include a color display and touch screen.

All DynaFlex models may also be purchased with an embedded barcode reader (BCR) and/or kiosk back cover options.

DynaFlex can be used in both attended and unattended environments. The Kiosk model includes a back cover that allows for secure mounting. All are approved as Secure Card Reader (SCR) devices, adhering to PCI PTS POI v5.1 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 2-9 below**.

NOTICE
Do not remove or alter this label.

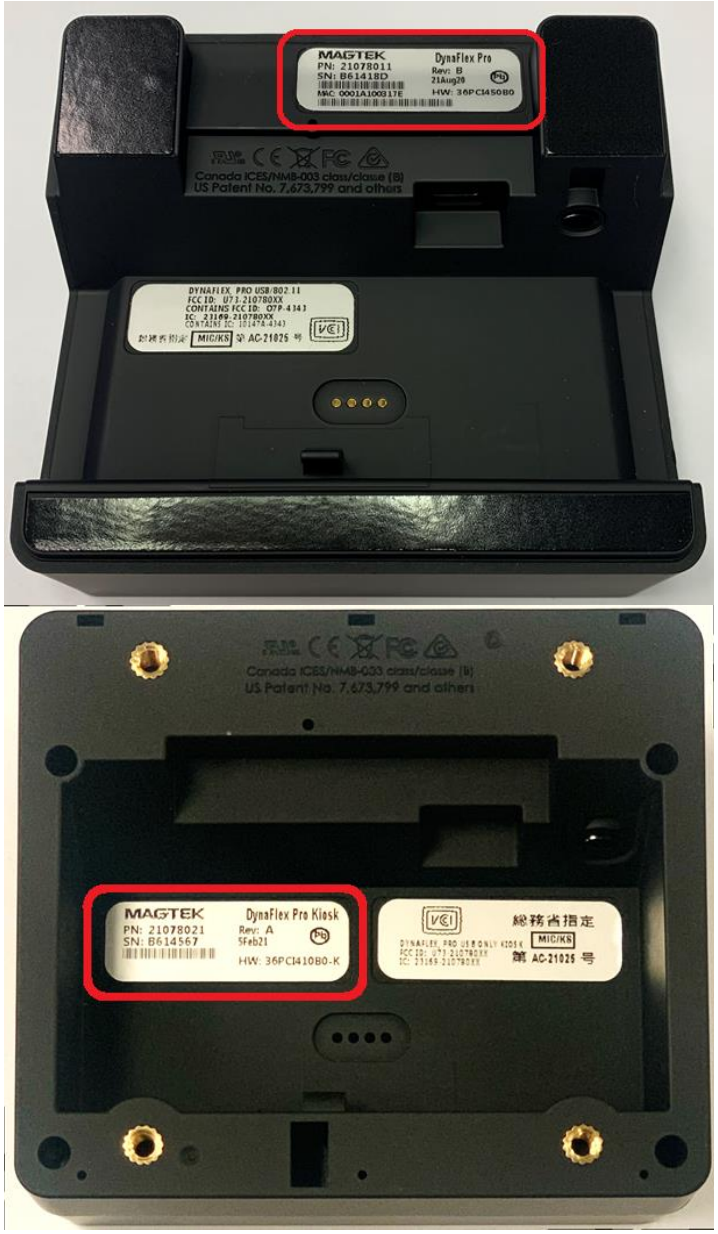


Figure 2-9 - DynaFlex Products Device Label Location

The printed label includes the following elements of device identification information, shown by the numbered callouts in **Figure 2-10**:

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

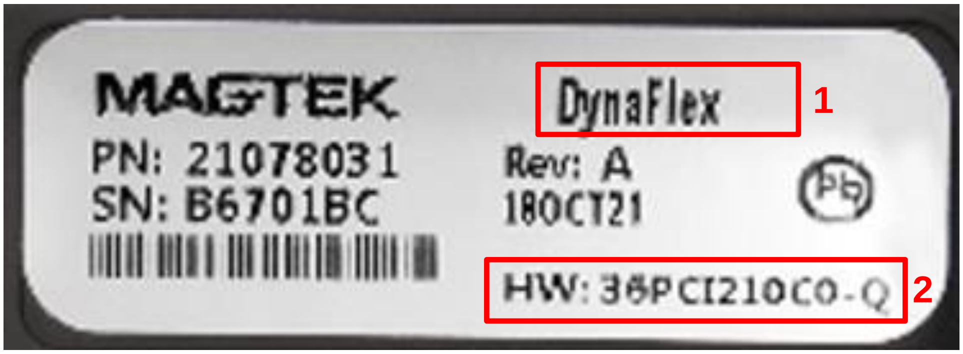


Figure 2-10 -DynaFlex / DynaFlex Pro Device Labels

The label also contains other supporting information about the device.

All DynaFlex product family hardware configurations are listed in **Table 2-1 - PCI Hardware Identifier** 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** **36PCI21xCx** **36PCI21xDx** **36PCI21xCx-Q** **36PCI21xDx-Q**	DynaFlex, No Display, USB
36PCI41xAx **36PCI41xBx** **36PCI41xCx** **36PCI41xDx** **36PCI41xCx-Q** **36PCI41xDx-Q**	DynaFlex Pro, Touchscreen Display, USB
36PCI21xBx-K **36PCI21xCx-K** **36PCI21xDx-K** **36PCI21xCx-KQ** **36PCI21xDx-KQ**	DynaFlex Kiosk, No Display, USB
36PCI41xBx-K **36PCI41xCx-K** **36PCI41xDx-K** **36PCI41xCx-KQ** **36PCI41xDx-KQ**	DynaFlex Pro Kiosk, Touchscreen Display, USB

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

Hardware Versions with Description of Associated Variables													
PCI Hardware ID Number	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
	3	6	P	C	I	2	1	x	A	x			
	3	6	P	C	I	2	1	x	B	x			
	3	6	P	C	I	2	1	x	C	x			
	3	6	P	C	I	2	1	x	D	x			
	3	6	P	C	I	2	1	x	C	x	-	Q	
	3	6	P	C	I	2	1	x	D	x	-	Q	
	3	6	P	C	I	4	1	x	A	x			
	3	6	P	C	I	4	1	x	B	x			
	3	6	P	C	I	4	1	x	C	x			
	3	6	P	C	I	4	1	x	D	x			
	3	6	P	C	I	4	1	x	C	x	-	Q	
	3	6	P	C	I	4	1	x	D	x	-	Q	
	3	6	P	C	I	2	1	x	B	x	-	K	
	3	6	P	C	I	2	1	x	C	x	-	K	
	3	6	P	C	I	2	1	x	D	x	-	K	
	3	6	P	C	I	2	1	x	C	x	-	K	Q
	3	6	P	C	I	2	1	x	D	x	-	K	Q
	3	6	P	C	I	4	1	x	B	x	-	K	
	3	6	P	C	I	4	1	x	C	x	-	K	
	3	6	P	C	I	4	1	x	D	x	-	K	
	3	6	P	C	I	4	1	x	C	x	-	K	Q
	3	6	P	C	I	4	1	x	D	x	-	K	Q

Fixed Position	Variable "X" Position	Description of Fixed or Variable "X" in the Selection Position
1-2		36 = DynaFlex
3-5		PCI = PCI Hardware
6		Front options 2 = NO Display 4 = Touchscreen Display
7		Interface Options 1 = USB only
	8	Cover Color: 0 = Black
9		Version A, B ,C and D = as Certified
	10	minor fixes not adding functionality or related to security (e.g., change component value for antenna matching): 0 = as certified
11-13		Additional Features -K = Kiosk Mounting -Q = Includes Barcode Reader -KQ = Kiosk Mounting with Barcode Reader Blank Spaces = NO Added Features

2.3.2 Firmware Identification

The most recent firmware versions for DynaFlex products are **1000007183-CAx-PCI** for the core firmware (Main FW) and **1000007536-Ax-PCI** for the secure bootloader (Boot1 FW). The lowercase x in firmware 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 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 at any time using ***Command 0xD101 Get Property*** as described in ***D998200383 DynaFlex and DynaFlex Pro Programmer's Manual (COMMANDS)***.

Note: MagTek will now use a two-character major revision designation when a new revision is released. For example, DynaFlex Devices will have revision designations that increase in length from older to newer, **Cx** → **CAx** → **CBx**.

Table 2-3 - Main Firmware Version and Associated Variables

<table>
<tr><th colspan="2" rowspan="2">Firmware Number</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th></tr>
<tr><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>7</td><td>1</td><td>8</td><td>3</td><td>-</td><td>C</td><td>A</td><td>x</td><td>-</td><td>P</td><td>C</td><td>I</td></tr>
<tr><th colspan="20">Main FW</th></tr>
<tr><th>Fixed Position</th><th>Variable "x" Position</th><th colspan="18">Description of Fixed or Variable "x" in the Selected Position</th></tr>
<tr><td>1-10</td><td></td><td colspan="18">1000007183 = DynaFlex Main firmware part number</td></tr>
<tr><td>12-13</td><td></td><td colspan="18">CA = Certified Version</td></tr>
<tr><td></td><td>14</td><td colspan="18">Minor revisions, bug fixes</td></tr>
<tr><td>16-18</td><td></td><td colspan="18">PCI = PCI version of firmware</td></tr>
</table>

Table 2-4 – Legacy Main Firmware and Associated Variables (17 Position)

<table>
<tr><th colspan="2" rowspan="2">Firmware Number</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th></tr>
<tr><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>7</td><td>1</td><td>8</td><td>3</td><td>-</td><td>C</td><td>x</td><td>-</td><td>P</td><td>C</td><td>I</td></tr>
<tr><th colspan="19">Legacy Main FW</th></tr>
<tr><th>Fixed Position</th><th>Variable "x" Position</th><th colspan="17">Description of Fixed or Variable "x" in the Selected Position</th></tr>
<tr><td>1-10</td><td></td><td colspan="17">1000007183 = DynaFlex Main firmware part number</td></tr>
<tr><td>12</td><td></td><td colspan="17">A, B or C = Certified Version</td></tr>
<tr><td></td><td>13</td><td colspan="17">Minor revisions, bug fixes</td></tr>
<tr><td>15-17</td><td></td><td colspan="17">PCI = PCI version of firmware</td></tr>
</table>

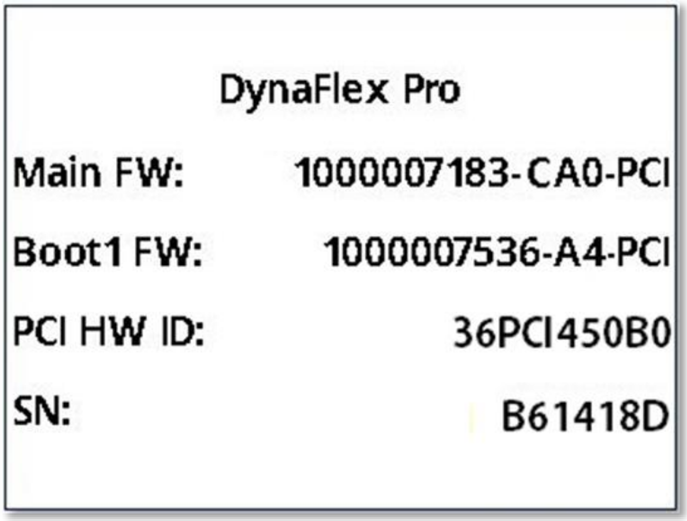
Table 2-5 - Boot Firmware Version and Associated Variables

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	7	5	3	6	-	A	x	-	P	C	I
Boot FW																	

Fixed Position	Variable "x" Position	Description of Fixed or Variable "x" in the Selected Position
1-10		1000007536 = DynaFlex Boot firmware part number
12		A = Certified Version
	13	Minor revisions, bug fixes
15-17		PCI = PCI version of firmware

2.3.3 Device Information Page

While powering up, DynaFlex models with a Touchscreen, display a startup page that includes the firmware versions installed on the device, see **Figure 2-11 - DynaFlex Pro Models Startup Screen,** 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.'



DynaFlex Pro

Main FW: 1000007183-CA0-PCI

Boot1 FW: 1000007536-A4-PCI

PCI HW ID: 36PCI450B0

SN: B61418D

Figure 2-11 - 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 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) 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. Compare the Hardware ID and Firmware ID: https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices
4) Check the Device S/N and make sure it matches with labels on shipping materials and documentation.
5) 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.
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 see **Figure 3-1 - Unobstructed View of Card Insertion Slot and Card Swipe Path**. This is intended to allow cardholders to easily detect suspicious objects in or around the card paths, such as bugs / skimmers / tapping mechanisms, 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.

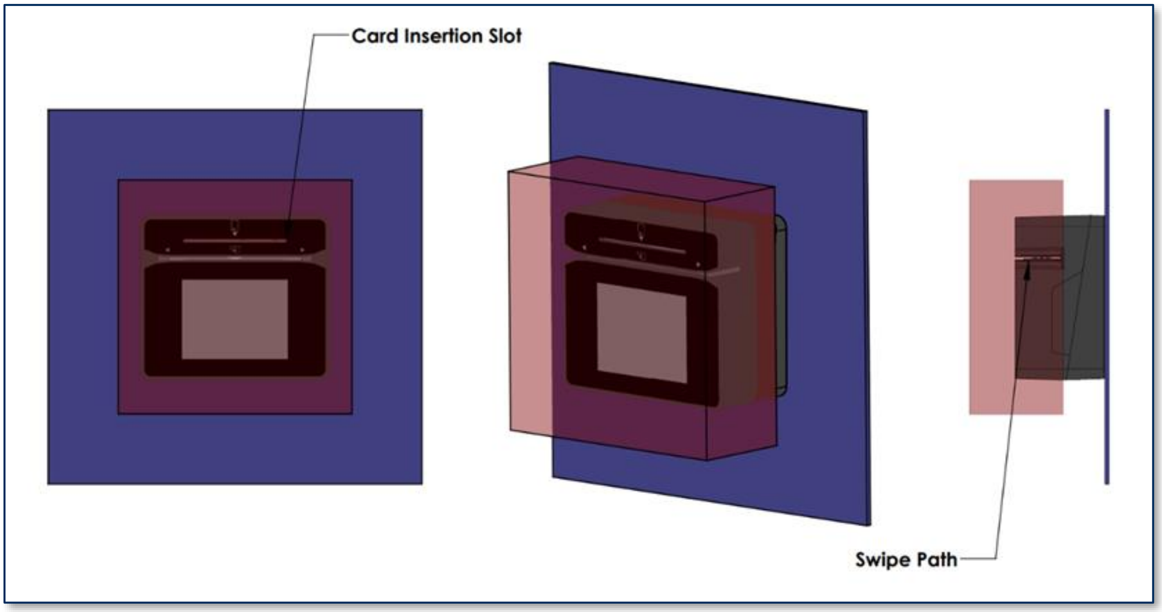


Figure 3-1 - Unobstructed View of Card Insertion Slot and Card Swipe Path

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.

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

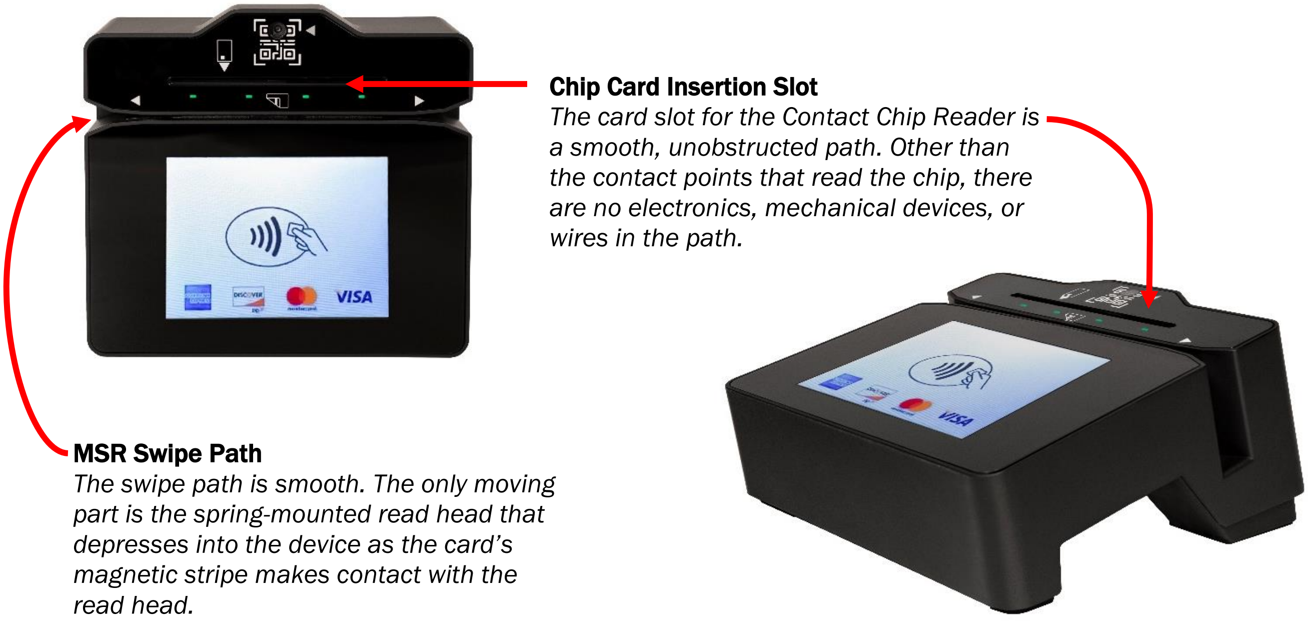
DynaFlex products ship from the factory fully secure. The devices have no configuration settings that require modification by the user to meet PCI security requirements.

4 Operation and Maintenance

4.1 Periodic Inspection

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

1) Evaluate the appearance of the secure card reader to make sure it is the correct product.
2) Inspect whether the MSR card slot has an additional card reader or inserted bugs. See **Figure 4-1**, below.
3) Observe the slot of smart card reader, inspect to see if 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) Power on the secure card reader and ensure 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.



Chip Card Insertion Slot
The card slot for the Contact Chip Reader is a smooth, unobstructed path. Other than the contact points that read the chip, there are no electronics, mechanical devices, or wires in the path.

MSR Swipe Path
The swipe path is smooth. The only moving part is the spring-mounted read head that depresses into the device as the card's magnetic stripe makes contact with the read head.

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 ***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 DynaFlex 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 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 flashing all four LEDs red. Devices equipped with a touchscreen will display "OFFLINE Tampered" when a tamper is triggered, all four LED indicators will also flash red, see **Figure 4-2 Tamper Response**. 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.

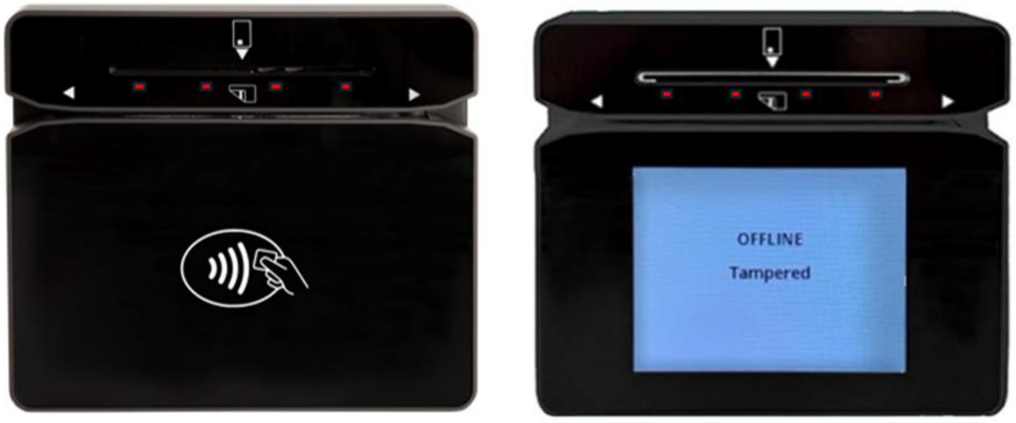


Figure 4-2 Tamper Response

4.6 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

DynaFlex 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 includes the following cryptographic algorithms:

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

Note: AES/DUKPT is not supported on older devices.

5.3 Key Management

DynaFlex 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 Products 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
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

5.4 Key Loading

DynaFlex 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.

5.5 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
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:

- ***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***