MAGTEK®
SECURITY FROM THE INSIDE

DynaFlex II

Secure Card Reader

PCI PTS POI v6.2 Security Policy

June 2023

Document Number:
D998200573-14

REGISTERED TO ISO 9001:2015

Table 0-1 - Revisions

Rev Number	Date	Notes
10	Mar 13, 2023	Initial Release
11	Apr 26, 2023	Add AES-256 to data protection algorithms Section 6.1
12	May 04, 2023	Add a picture showing the bottom view of device with both BCR and Kiosk options.
13	May 10, 2023	Adjust description for Secure Card Reader and update references.
14	June 5, 2023	Remove some wording in the preface. Remove mention of a display and add detail on retrieving firmware version.

Table of Contents

1 Purpose

This document describes how to use **DynaFlex II** 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 views of **DynaFlex II** and **DynaFlex II** with **Barcode Reader (BCR) option,** are shown in **Figure 2-1 below**. The different bottom views of all device options are shown in **Figure 2-3**.

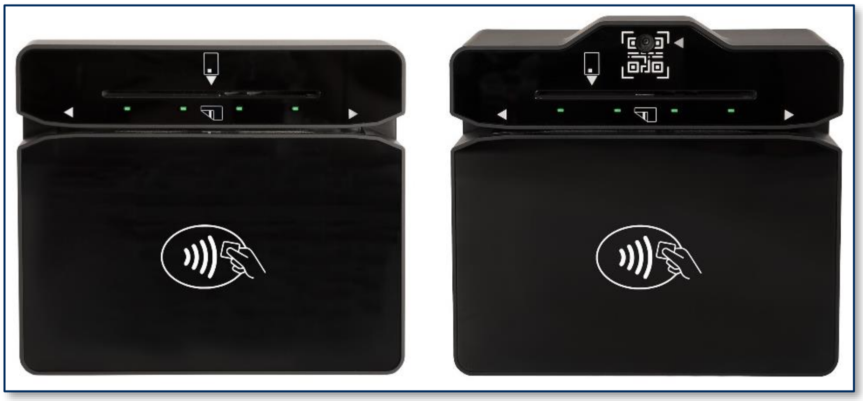


Figure 2-1 – Front Views of DynaFlex II and DynaFlex II (BCR)

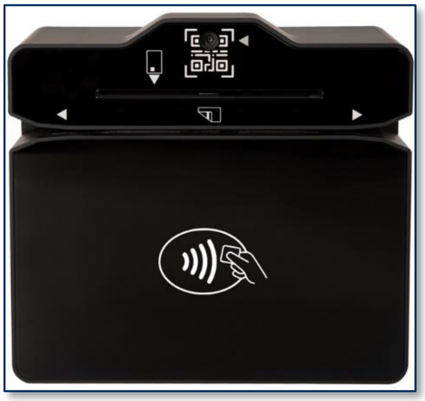


Figure 2-2 - Front View of DynaFlex II (Kiosk BCR)

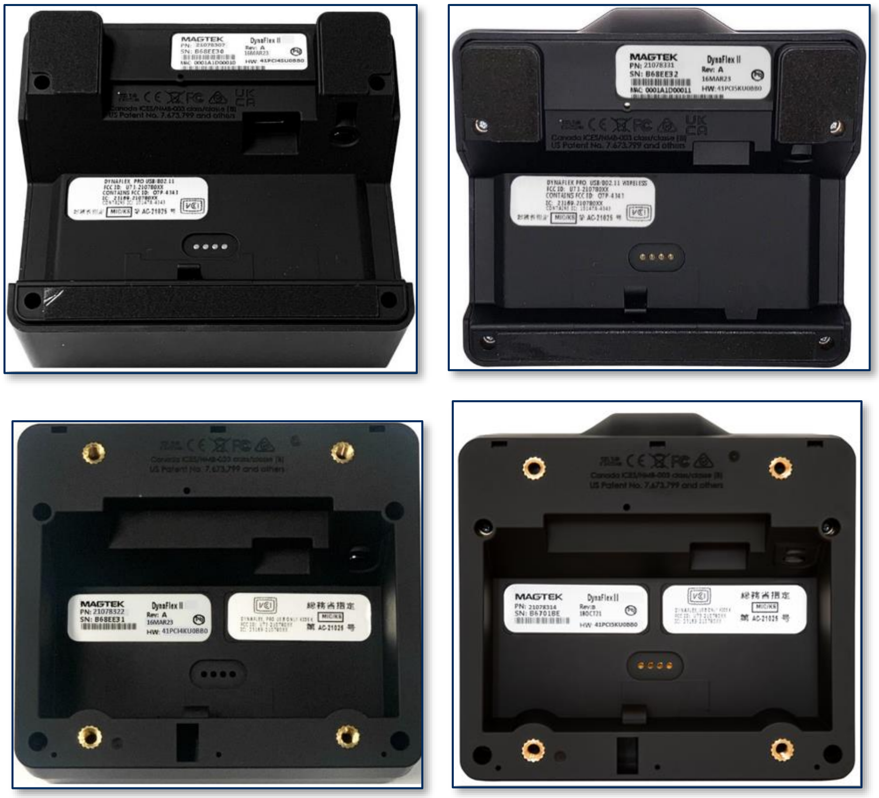


Figure 2-3 – Bottom Views for DynaFlex II, DynaFlex II (BCR), DynaFlex II (Kiosk), and DynaFlex II (Kiosk BCR)

3 Product Type

DynaFlex II includes USB communications, magnetic stripe readers (MSR), contact chip card reader (ICCR), and contactless card reader (CTLS). DynaFlex II may also be purchased with an embedded barcode reader (BCR) and/or kiosk back cover options.

DynaFlex II can be used as a desktop or handheld reader. The Kiosk version uses a back cover that allows for secure mounting, suitable for use in an unattended environment. All are approved as Secure Card Reader (SCR) devices, adhering to PCI PTS POI v6.2 requirements. Usage in any other environment will invalidate the approval.

3.1 Identification

3.1.1 Hardware Identification

To find important product identification, look on the printed product label on the bottom of the device as shown in **Figure 3-1** 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.

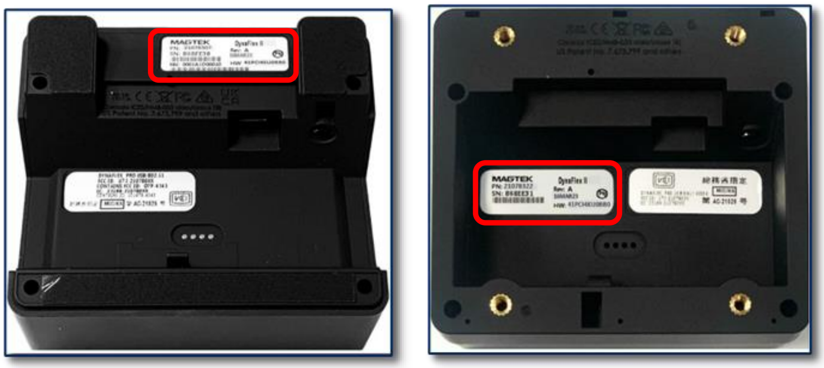


Figure 3-1 - DynaFlex II Device Label Locations

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

1) Product model name
2) PCI Hardware Identifier (“HW”)

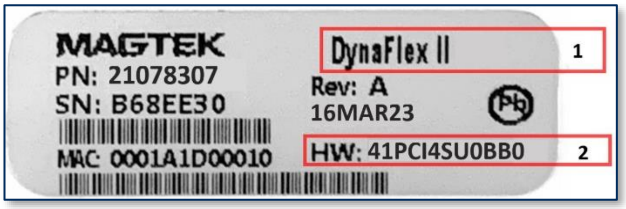


Figure 3-2 - DynaFlex II Device Label

The label also contains other supporting information about the device.

All DynaFlex II hardware configurations are listed **below**:

Table 3-1 - PCI Hardware Identifier

PCI ID Tag	Configuration Description
41PCI4SU0xBx	DynaFlex II, USB
41PCI5SU0xBx	DynaFlex II, BCR, USB
41PCI4KU0xBx	DynaFlex II, Kiosk, USB
41PCI5KU0xBx	DynaFlex II, Kiosk, BCR, USB

Table 3-2 – Hardware Versions with Description of Associated Variables

<table>
<tr><th colspan="14">Hardware Versions with Description of Associated Variables</th></tr>
<tr><td colspan="2" rowspan="5"><b>PCI Hardware ID Number</b></td><td><b>1</b></td><td><b>2</b></td><td><b>3</b></td><td><b>4</b></td><td><b>5</b></td><td><b>6</b></td><td><b>7</b></td><td><b>8</b></td><td><b>9</b></td><td><b>10</b></td><td><b>11</b></td><td><b>12</b></td></tr>
<tr><td>4</td><td>1</td><td>P</td><td>C</td><td>I</td><td>4</td><td>S</td><td>U</td><td>0</td><td>x</td><td>B</td><td>x</td></tr>
<tr><td>4</td><td>1</td><td>P</td><td>C</td><td>I</td><td>5</td><td>S</td><td>U</td><td>0</td><td>x</td><td>B</td><td>x</td></tr>
<tr><td>4</td><td>1</td><td>P</td><td>C</td><td>I</td><td>4</td><td>K</td><td>U</td><td>0</td><td>x</td><td>B</td><td>x</td></tr>
<tr><td>4</td><td>1</td><td>P</td><td>C</td><td>I</td><td>5</td><td>K</td><td>U</td><td>0</td><td>x</td><td>B</td><td>x</td></tr>
<tr><th>Fixed Position</th><th>Variable “X” Position</th><th colspan="12">Description of Fixed or Variable “X” in the Selection Position</th></tr>
<tr><td><b>1-2</b></td><td></td><td colspan="12">41 = DynaFlex II (certified SCR)</td></tr>
<tr><td><b>3-5</b></td><td></td><td colspan="12">PCI = PCI Hardware</td></tr>
<tr><td><b>6</b></td><td></td><td colspan="12">Front options
4 = Standard
5 = includes Barcode Reader</td></tr>
<tr><td><b>7</b></td><td></td><td colspan="12">Back options
S = Standard
K = Kiosk Mounting</td></tr>
<tr><td><b>8</b></td><td></td><td colspan="12">Interface Options
U = USB</td></tr>
<tr><td><b>9</b></td><td></td><td colspan="12">Placeholder
0 = As certified.</td></tr>
<tr><td></td><td><b>10</b></td><td colspan="12">Cover Color:
B = Black
G = Gray
W = White</td></tr>
<tr><td><b>11</b></td><td></td><td colspan="12">Version
B = as Certified</td></tr>
<tr><td></td><td><b>12</b></td><td colspan="12">minor fixes not adding functionality or related to security (e.g. change component value for antenna matching):
0 = as certified</td></tr>
</table>

3.1.2 Firmware Identification

The most recent firmware versions for DynaFlex II is **1000009341-A0-PCI** for the secure bootloader (Boot FW) and **1000009335-A1-PCI** for the core firmware (Main 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 listed on the PCI Approved Devices website. Note that in PCI listings, lowercase "x" is a wildcard meaning 'any single character.'

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)***.

Table 3-3 - 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
	1	0	0	0	0	0	9	3	3	5	-	A	x	-	P	C	I

Main FW		
Fixed Position	**Variable "x" Position**	**Description of Fixed or Variable "x" in the Selected Position**
1-10		1000009335 = DynaFlex II main firmware part number
12		A = Certified Version
	13	Minor revisions, bug fixes
15-17		PCI = PCI version of firmware

Table 3-4 – 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	9	3	4	1	-	A	x	-	P	C	I

Boot FW		
Fixed Position	**Variable "x" Position**	**Description of Fixed or Variable "x" in the Selected Position**
1-10		1000009341 = DynaFlex II Boot firmware part number
12		A = Certified Version
	13	Minor revisions, bug fixes
15-17		PCI = PCI version of firmware

4 Installation and User Guidance

4.1 Initial Inspection

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

1) Check the Device S/N and make sure it matches with labels on shipping materials and documentation.
2) Visually inspect the device, per ***D998200563 DynaFlex II Device Inspection or D998200566 DynaFlex II KIOSK Device Inspection***, which is included in the package with each device.
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 retrievable from the device via command. Go to the PCI compliance web page and search for MagTek, and find the product name, DynaFlex II. Compare the Hardware ID and Firmware ID: https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices
4) Inspect the label found on the bottom of the device (see section **3.1.1 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.
5) Follow the steps in **section 3.1.2** to retrieve 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. Note that in PCI listings, lowercase "x" is a wildcard meaning 'any single character.

4.2 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.

DynaFlex II 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 with kiosk back cover, it is important that the device 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 4-1 - Unobstructed View of Card Insertion Slot and Card Swipe Path**. This will ensure that the cardholder can easily identify suspicious objects in or around the card paths, such as bugs / skimmers / tapping mechanisms, and wires or antennas. Installation height is one factor in meeting this requirement. DynaFlex II 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.

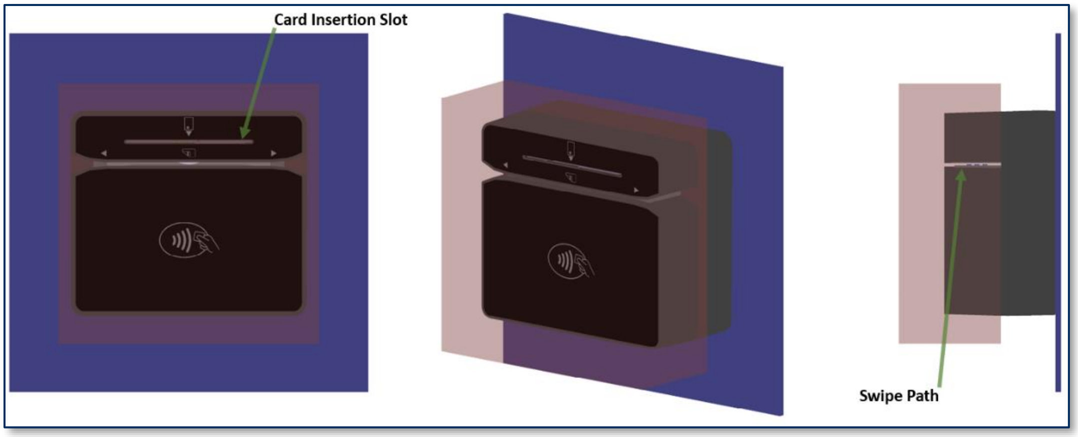


Figure 4-1 - Unobstructed View of Card Insertion Slot and Card Swipe Path

4.3 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

⚠ CAUTION

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 4-1 - 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

4.4 Communications and Security Protocols

DynaFlex II supports 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.

4.5 Configuration Settings

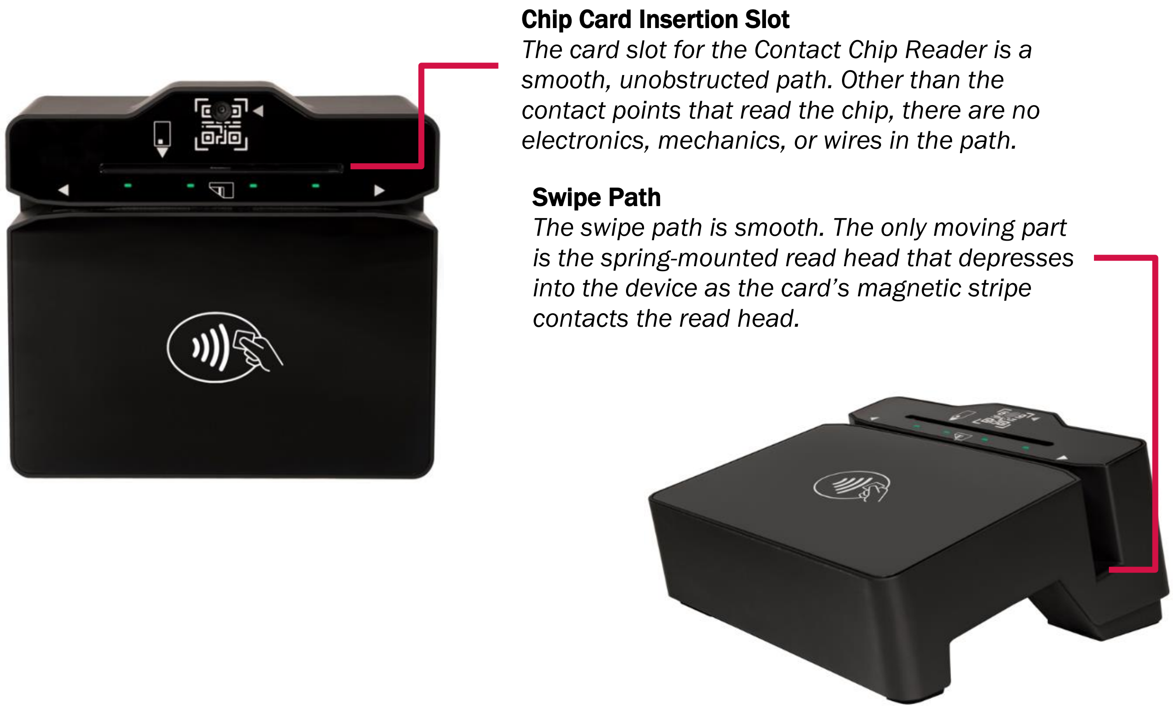
DynaFlex II ships from the factory fully secure. The devices have no configuration settings that require modification by the user to meet PCI security requirements.

5 Operation and Maintenance

5.1 Periodic Inspection

The merchant or end user, should inspect the appearance of secure card reader daily, paying close attention to the following:

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 5-1**, below.
3) Observe the Chip Card Insertion Slot to determine whether there are any wires or obstructions. See **Figure 5-1,** below.
4) Inspect whether the product's appearance has been altered.
5) Check if the firmware version is correct.
6) 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.



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, mechanics, or wires in the path.

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 contacts the read head.

Figure 5-1 - Chip Card Insertion Slot and Swipe Path Examples

MagTek strongly recommends performing security inspections on a regular schedule. Additional information can be found in ***D998200563 DYNAFLEX II DEVICE INSPECTION*** or ***D998200566 DYNAFLEX II 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.

5.2 Self-Test

DynaFlex II 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.

5.3 Roles and Responsibilities

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

5.4 Passwords and Certificates

DynaFlex II 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.

5.5 Tamper Response

If the device senses a physical or environmental attack, it erases all sensitive keys, and will have limited functionality. While powered on, DynaFlex II indicates the tampered state has been triggered by flashing all four LEDs red (see **Figure 5-2 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.

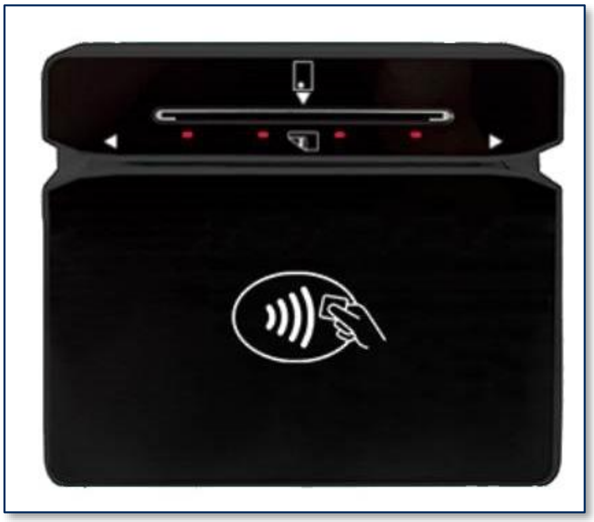


Figure 5-2 Tamper Response

5.6 Patching and Updating

DynaFlex II 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.

5.7 Decommissioning

Before DynaFlex II 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.

6 Security

6.1 Account Data Protection

DynaFlex II always encrypts account data from all three reader types, 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.

6.2 Algorithms Supported

The device uses the following cryptographic algorithms:

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

6.3 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.***

Table 6-1 - DynaFlex II Product Keys

Key Name	Size	Algorithm	Purpose
Transport Keys	32 bytes	AES TR-31 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	ECC-DSA SHA-256	Checks integrity and authenticity of firmware
EMV CA Public keys	Varies per issuer	RSA	Authenticate card data and keys

6.4 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.

6.5 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***.

7 Acronyms

Table 7-1 - Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
BCR	Barcode Reader
BLE	Bluetooth Low Energy
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
POI	Point Of Interaction
S/N	Serial Number
SCR	Secure Card Reader
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)***
- ***D998200563 DynaFlex II Device Inspection***
- ***D998200566 DynaFlex II Kiosk Products Device Inspection***
- ***D998200564 DynaFlex II Family Package Inspection***
- ***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***
- ***ANSI X9.143-2022, Interoperable Secure Key Exchange Key Block Specification***