MAGTEK®
SECURITY FROM THE INSIDE

iDynamo 5 Gen III

Secure Card Reader

PCI PTS POI v6.2 Security Policy

April 2024

Document Number:
D998200619-101

REGISTERED TO ISO 9001:2015

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

Table 0-1 - Revisions

Rev Number	Date	Notes
100	February 02, 2024	Initial Release
101	April 9, 2024	Update section **2.3.2 Firmware Identification** to remove all references to HEX txt.

Table of Contents

1 Purpose

This document addresses the proper use of iDynamo 5 Gen III secure card readers (SCR), in a secure manner. This includes information about key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements.

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

Throughout this document:

- **iDynamo 5 Gen III** refers to all products in the iDynamo 5 Gen III product family.

2 General Description

2.1 Product Name and Appearance

The front view of iDynamo 5 Gen III, is shown in **Figure 2-1 below**. The back view of iDynamo 5 Gen III is shown in **Figure 2-2**. The side views of iDynamo 5 Gen III can be seen in **Figure 2-3** and **Figure 2-4**. The Top View displaying the pushbutton and LED indicator can be seen in **Figure 2-5**, and the Bottom View displaying the USB-C receptacle can be seen in **Figure 2-6**.

Figure 2-1 –Front View

Figure 2-2 – Back View

Figure 2-3 - Left Side View

Figure 2-4 - Right Side View

Figure 2-5 - Top View

Figure 2-6 - Bottom View

2.2 Product Type

iDynamo 5 Gen III devices include a USB-C interface for Power and Communications, and a magnetic stripe reader (MSR).

iDynamo 5 Gen III can be used as a desktop or handheld device. It is approved as a secure card reader (SCR) 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 information, look for the printed product label on the back face of the device as shown in **Figure 2-7 below**.

NOTICE
Do not remove or alter this label.

Figure 2-7 – iDynamo 5 Gen III Device Label Location

The product label includes the following elements of device identification information, shown by the numbered callouts in **Figure 2-8**.

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

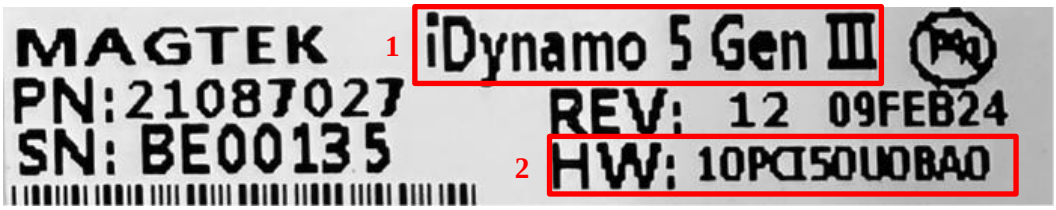

Figure 2-8 -iDynamo 5 Gen III Device Label

The label also contains other supporting information about the device.

All iDynamo 5 Gen III hardware configurations are listed in **Table 2-1 below**. The device utilizes one interface type, **USB-C**. Use of any interface other than USB-C will invalidate PCI approval.

Table 2-1 - PCI Hardware Identifier

PCI ID Tag	Configuration Description
10PCI50U0BA0	iDynamo 5 Gen III, PCI, BLACK

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**
	1	**0**	**P**	**C**	**I**	**5**	**0**	**U**	**0**	**B**	**A**	**0**

Fixed Position	Variable "X" Position	Description of Fixed or Variable "X" in the Selection Position
1-2		10 = iDynamo 5 Gen III
3-5		PCI = PCI Hardware
6		Device Options 5 = Standard
7		Option RFU (Reserved for Future Use) RFU 0 = as Certified
8		Interface Options U = USB
9		Option RFU (Reserved for Future Use) RFU 0 = as Certified
	10	Cover Color: B = Black
11		Version A = 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 iDynamo 5 Gen III products are **1000009547-AA1-PCI** for the secure bootloader, and **1000009546-ADB-PCI** for the core firmware (Main - BIN). The lowercase x in firmware versions indicates minor non-security related changes, see **Table 2-3** and **Table 2-4**.

Table 2-3 - 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	18
	1	0	0	0	0	0	9	5	4	6	-	A	D	x	-	P	C	I
Main FW																		
Fixed Position	**Variable "x" Position**	**Description of Fixed or Variable "x" in the Selected Position**																
1-10		1000009421 = iDynamo 5 Gen III Main Firmware Part Number																
11		Delimiter (-)																
12-13		AD = Certified Version																
	14	Minor Revisions, Bug Fixes																
15		Delimiter (-)																
16-18		PCI = PCI Version of Firmware																

Table 2-4 - 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	18
	1	0	0	0	0	0	9	5	4	7	-	A	A	x	-	P	C	I
Boot FW																		
Fixed Position	**Variable "x" Position**	**Description of Fixed or Variable "x" in the Selected Position**																
1-10		1000009446 = iDynamo 5 Gen III Boot Firmware Part Number																
11		Delimiter (-)																
12-13		AA = Certified Version																
	14	Minor Revisions, Bug Fixes																
15		Delimiter (-)																
16-18		PCI = PCI Version of Firmware																

All device identification information, including firmware versions and PCI Hardware ID, is accessible by connecting iDynamo 5 Gen III to a host device via USB-C using the latest software provided by MagTek, as seen in **Figure 2-9 - Device Information Screen**.

The host user can retrieve device information at any time using ***Command 0xD101 Get Property*** as described in ***D998200587 iDynamo 5 Gen III Programmer's Manual COMMANDS***.

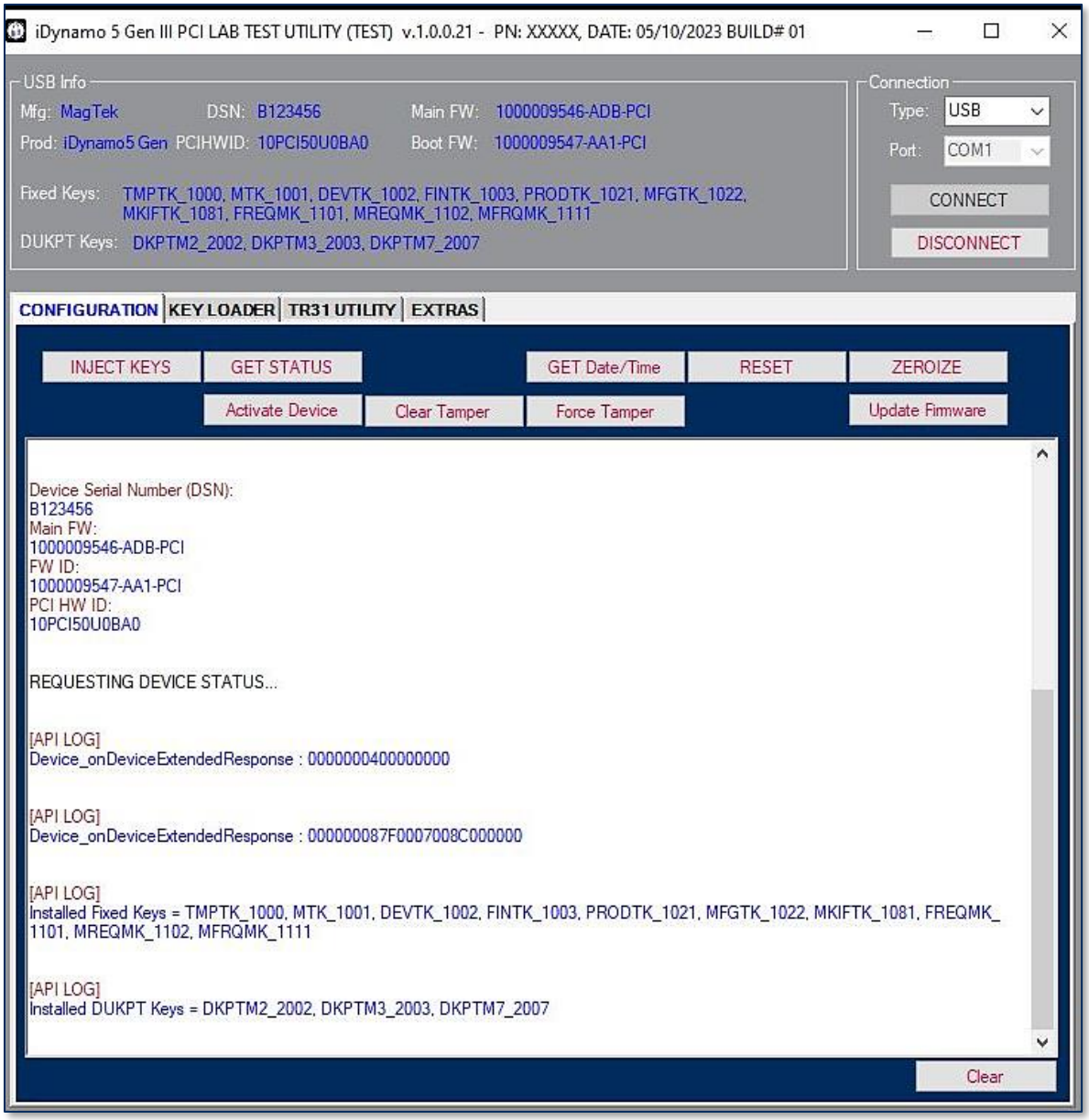

Figure 2-9 - Device Information Screen

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 the **Hardware #** listed for the device on the PCI website for Approved Devices. Go to the PCI compliance web page and search for MagTek, and find the product name, iDynamo 5 Gen III. Compare the Hardware ID and Firmware ID:
   https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

   Note: Firmware ID is accessible by connecting iDynamo 5 Gen III to a host device via USB-C, using the latest software provided by MagTek (see section **2.3.2 Firmware Identification**).
3) Check the Device serial number (SN) and make sure it matches with labels on shipping materials and documentation.
4) Visually inspect the device, per ***D998200620 iDynamo 5 (Gen III) SRED, Device Inspection Manual***, which is included in the package with each device. See section **4.1 Periodic Inspection** for more information regarding visual inspection of the device.
5) 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 iDynamo 5 Gen III. Note that in PCI listings, lowercase "x" is a wildcard meaning 'any single character.'

3.2 Installation

Connect the device to a host via USB-C for control and power. iDynamo 5 Gen III products are designed to provide flexible mounting options such as:

- External clip
- Embedded lanyard

3.3 Environmental Conditions

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

- Operating temperature range: 32°F to 95°F (0°C to 35°C) 5-90% RH with no condensation
- Storage temperature range: -4°F to 113°F (-20°C to 45°C) 10-90% RH with no condensation

Any temperature or operating voltage outside the values listed above 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.

3.4 Communications and Security Protocols

iDynamo 5 Gen III products support a USB-C interface using the USB-HID protocol. Transactions, configuration, firmware updates, and key injection can all be performed using this interface type. Use of any method not listed in this security policy will invalidate the device's PCI PTS approval.

3.5 Configuration Settings

iDynamo 5 Gen III 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 on a daily basis:

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) Inspect whether the product appearance has been changed.
4) Check if the firmware version is correct.
5) After connecting the device to a USB-C power supply, it will power on, the LED indicator should illuminate green and remain powered on to indicate the device is in an idle state, ready for a transaction. Powering on the secure card reader will test hardware security and authenticity, and the integrity of the installed firmware.

Figure 4-1 - Card Swipe Path Example

MagTek strongly recommends performing security inspections on a regular schedule. Additional information can be found in ***D998200620 iDynamo 5 (Gen III) SRED, Device Inspection Manual***. 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

iDynamo 5 Gen III performs self-tests at power-up and after reset. The device automatically resets and performs self-tests every 24 hours at the configured time of day. No manual intervention by the operator is 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

iDynamo 5 Gen III 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 a tampered state by illuminating its only LED solid red, as seen in **Figure 4-2 Tamper Response**. If this occurs:

1) Remove the device from service immediately.
2) Store it securely for a 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

iDynamo 5 Gen III 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-C interface 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.

4.7 Decommissioning

Before iDynamo 5 Gen III 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 back 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 112-bit TDEA, 128-bit AES, or 256-bit AES 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
- ECDSA (P256 and P521 curves)
- SHA-256

5.3 Key Management

The device implements the original 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 - iDynamo 5 Gen III Product 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

5.4 Key Loading

The device does not support manual or plaintext 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
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:

- ***D998200614 iDynamo 5 Gen III Installation and Operation Manual***
- ***D998200587 iDynamo 5 Gen III Programmer's Manual COMMANDS***
- ***D998200620 iDynamo 5 Gen III SRED, Device Inspection Manual***
- ***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***