MAGTEK®
SECURITY FROM THE INSIDE

DynaFlex II Go

Secure Card Reader

PCI PTS POI v6.2 Security Policy

October 2024

Document Number:
D998200596-110

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

Copyright © 2006 - 2024 MagTek, Inc.
Printed in the United States of America

MagTek® is a registered trademark of MagTek, Inc.
MagnePrint® is a registered trademark of MagTek, Inc.
MagneSafe® is a registered trademark of MagTek, Inc.
Magensa™ is a trademark of MagTek, Inc.

AAMVA™ is a trademark of AAMVA.
American Express® and EXPRESSPAY FROM AMERICAN EXPRESS® are registered trademarks of American Express Marketing & Development Corp.
Apple Pay® is a registered trademark to Apple Inc.
D-PAYMENT APPLICATION SPECIFICATION® is a registered trademark to Discover Financial Services CORPORATION
MasterCard® is a registered trademark and PayPass™ and Tap & Go™ are trademarks of MasterCard International Incorporated.
Visa® and Visa payWave® are registered trademarks of Visa International Service Association.

ANSI®, the ANSI logo, and numerous other identifiers containing "ANSI" are registered trademarks, service marks, and accreditation marks of the American National Standards Institute (ANSI).
ISO® is a registered trademark of the International Organization for Standardization.
PCI Security Standards Council® is a registered trademark of the PCI Security Standards Council, LLC.
EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC. The Contactless Indicator mark, consisting of four graduating arcs, is a trademark owned by and used with permission of EMVCo, LLC.
UL™ and the UL logo are trademarks of UL LLC.

All other system names and product names are the property of their respective owners.

Table 0-1 - Revisions

Rev Number	Date	Notes
100	October 25, 2023	Initial Release
101	November 21, 2023	Update **3.4 Communications and Security Protocols** with Bluetooth LE Secure Connections content , **Update 4.4 Passwords and Certificates** with Bluetooth LE Pass Key content.
102	December 20, 2023	Update **Table 2-3 - Main Firmware Version and Associated Variables**, **Table 2-4 - Boot Firmware Version and Associated Variables**, **Table 2-5 - Bluetooth LE Firmware Version and Associated Variables**
110	October 28, 2024	Update HW IDs in **2.3.1 Hardware Identification**; Update FW IDs and Added new ID for main FW with newer EMV Kernels in **2.3.2Firmware Identification**

Table of Contents

1 Purpose

This document addresses the proper use of the DynaFlex II Go family of 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:

- **DynaFlex II Go products** refers to all products in the DynaFlex II Go product family, including DynaFlex II Go models equipped with a barcode reader (BCR) and Bluetooth LE connectivity.

2 General Description

2.1 Product Name and Appearance

The front view of all DynaFlex II Go models (with and without BCR), are shown in **Figure 2-1 below**. The back view of all DynaFlex II Go devices are identical, as seen in **Figure 2-2**.

Figure 2-1 - DynaFlex II Go and DynaFlex II Go with BCR Front View

Figure 2-2 – Back View of all DynaFlex II Go Models

2.2 Product Type

All DynaFlex II Go products include USB communications, a magnetic stripe reader (MSR), a contact chip card reader (ICCR), a contactless card reader (CTLS), and may also be purchased with an embedded barcode reader (BCR) and Bluetooth LE connectivity.

DynaFlex II Go models can be used as desktop or handheld devices. They are 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, look on the printed product label on the back face of the device as shown in **Figure 2-3 below**.

NOTICE
Do not remove or alter this label.

Figure 2-3 - DynaFlex II Go Device Label Location

The product label includes the following elements of device identification information, indicated by the numbered callouts in **Figure 2-4** and **Figure 2-5**.

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

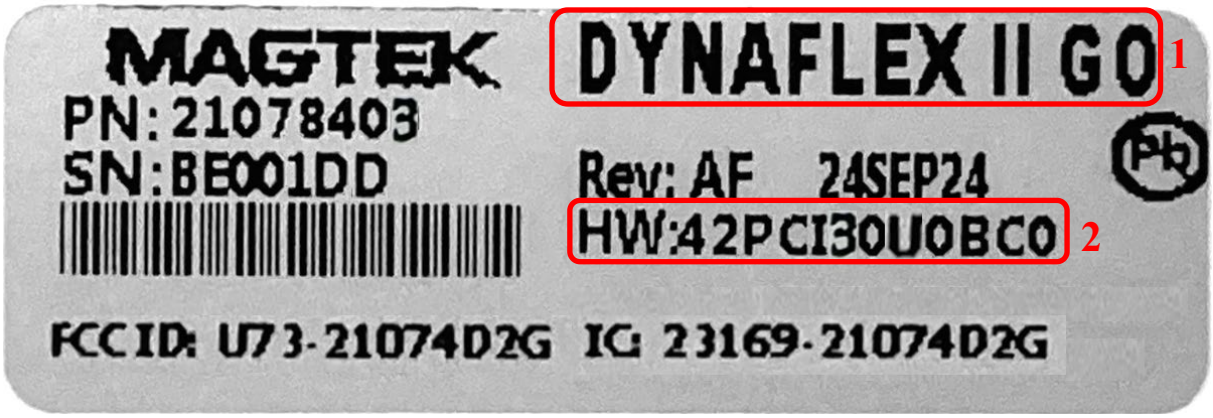

Figure 2-4 -DynaFlex II Go Device Label

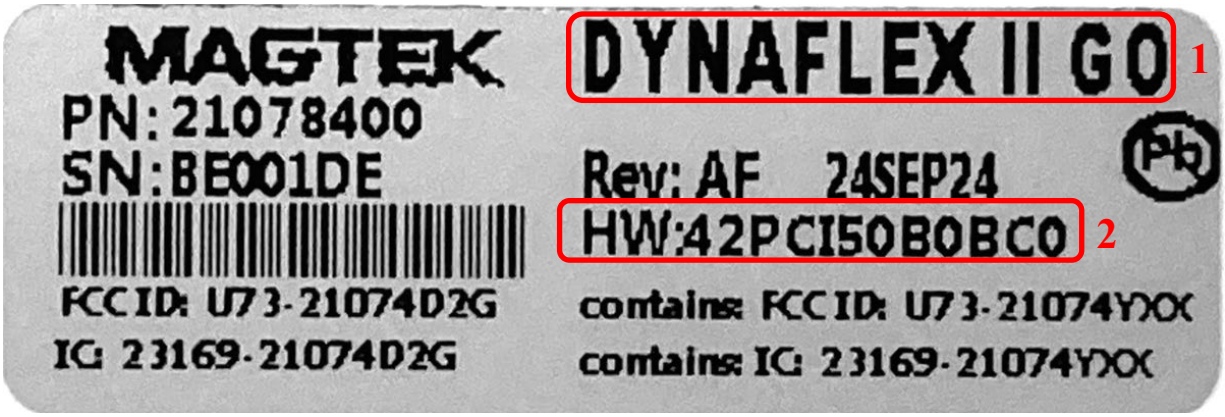

Figure 2-5 DynaFlex II Go with Bluetooth LE Device Label

The label also contains other supporting information about the device.

All DynaFlex II Go product family hardware configurations are listed in **Table 2-1 below**. The device utilizes two interface types, USB and Bluetooth LE. Use of any interface other than USB or Bluetooth LE will invalidate PCI approval.

Table 2-1 - PCI Hardware Identifier

PCI ID Tag	Configuration Description
42PCI30U0BB0	DynaFlex II Go, PCI, BLACK
42PCI50U0BB0	DynaFlex II Go, PCI, BCR, BLACK
42PCI30B0BB0	DynaFlex II Go, PCI, BLACK, BLUETOOTH LE
42PCI50B0BB0	DynaFlex II Go, PCI, BCR, BLACK, BLUETOOTH LE
42PCI30U0BC0	DynaFlex II Go, PCI, BLACK
42PCI50U0BC0	DynaFlex II Go, PCI, BCR, BLACK
42PCI30B0BC0	DynaFlex II Go, PCI, BLACK, BLUETOOTH LE
42PCI50B0BC0	DynaFlex II Go, PCI, BCR, BLACK, BLUETOOTH LE

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**
		4	2	P	C	I	3	0	U	0	B	B	0
		4	2	P	C	I	5	0	U	0	B	B	0
		4	2	P	C	I	3	0	B	0	B	B	0
		4	2	P	C	I	5	0	B	0	B	B	0
		4	2	P	C	I	3	0	U	0	B	C	0
		4	2	P	C	I	5	0	U	0	B	C	0
		4	2	P	C	I	3	0	B	0	B	C	0
		4	2	P	C	I	5	0	B	0	B	C	0
Fixed Position	**Variable "X" Position**	**Description of Fixed or Variable "X" in the Selection Position**											
1-2		42 = DynaFlex II Go											
3-5		PCI = PCI Hardware											
6		Front options 3 = Standard 5 = includes Barcode Reader											
7		Option RFU (Reserved for Future Use) RFU 0 = as Certified											
8		Interface Options U = USB only B = USB + Bluetooth LE											
9		Option RFU (Reserved for Future Use) RFU 0 = as Certified											
	10	Cover Color: B = Black											
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 Go products are **1000009446-AA0-PCI** for the secure bootloader (Boot1 FW), **1000009421-AB0-PCI** and **1000009714-AB0-PCI** for the core firmware (Main FW), and **1000009327-AA0-PCI** for the Bluetooth LE Firmware Version. The X in firmware versions indicates 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 and PCI Hardware ID, is accessible by connecting DynaFlex II Go to a host device via USB or Bluetooth LE, using the latest software provided by MagTek, as seen in **Figure 2-6 - Device Information Screen**.

The host user can also can retrieve device information at any time using ***Command 0xD101 Get Property*** as described in ***D998200597 DynaFlex II Go Programmer's Manual (COMMANDS)***.

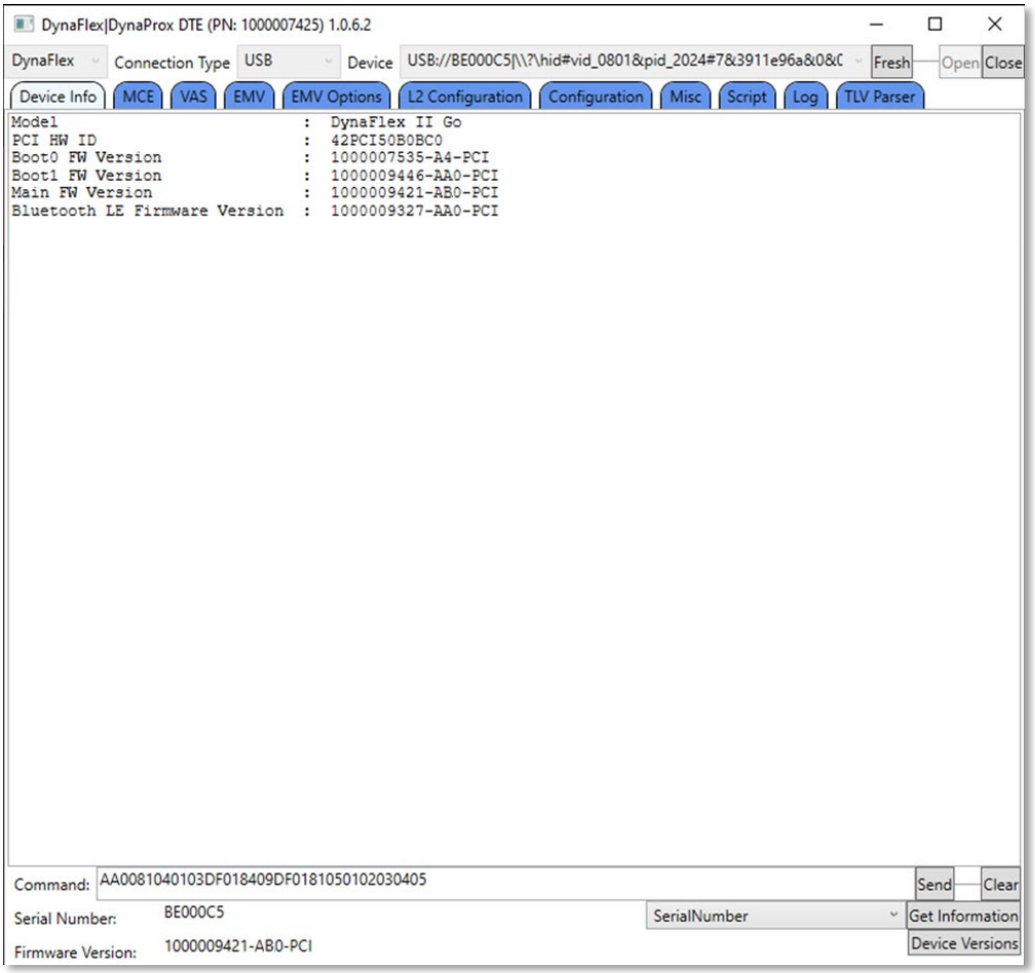

Figure 2-6 - Device Information Screen

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	4	2	1	-	A	A	x	-	P	C	I
	1	0	0	0	0	0	9	4	2	1	-	A	B	x	-	P	C	I
	1	0	0	0	0	0	9	7	1	4	-	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		1000009421, 1000009714 = DynaFlex II Go Main firmware part number
12-13		1000009421 - AA and AB = Certified Version 1000009714 - AB Certified Version
	14	Minor revisions, bug fixes
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	4	4	6	-	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 = DynaFlex II Go Boot firmware part number
12-13		AA = Certified Version
	14	Minor revisions, bug fixes
16-18		PCI = PCI version of firmware

Table 2-5 - Bluetooth LE 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	3	2	7	-	A	A	x	-	P	C	I

Bluetooth LE FW		
Fixed Position	**Variable "x" Position**	**Description of Fixed or Variable "x" in the Selected Position**
1-10		1000009327 = DynaFlex II Go Bluetooth LE firmware part number
12-13		AA = Certified Version
	14	Minor revisions, bug fixes
16-18		PCI = PCI version of firmware

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 web site for Approved Devices. Go to the PCI compliance web page and search for MagTek, and find the product name, DynaFlex II Go. Compare the Hardware ID and Firmware ID: https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

   Note: Firmware ID is accessible by connecting DynaFlex II Go to a host device via USB or Bluetooth LE, 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 ***D998200593 DynaFlex II Go, Device Inspection Document***, 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 DynaFlex II Go. 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 control and power (if battery power is not sufficient). DynaFlex II Go 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: 0°C to 35°C / 5% to 90% RH
- Storage temperature range: -20°C to 45°C / 5% to 90% RH

For safety, battery charging is disabled when the device is 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 II Go products support a USB interface using the USB-HID protocol, and a Bluetooth LE interface. Transactions, configuration, firmware updates, and key injection can all be performed using these interface types. Use of any method not listed in this security policy will invalidate the device's PCI PTS approval.

The device requires Bluetooth LE hosts to use version 4.2 or higher and use LE Security Mode 1 Level 4 (Secure Connections) only. "Just Works" cannot be used at any time. The device does not support or allow for the use of insecure communication options such as, but not limited to, LE Security Mode 2, and levels 1, 2, and 3 of LE Security Mode 1 and the "Just Works" secure pairing option of Security Mode 1.

3.5 Configuration Settings

DynaFlex II Go 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 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) 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 ***D998200593 DynaFlex II Go, Device Inspection Document***. 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 Go performs self-tests at power-up and after reset. By default, 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 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

DynaFlex II Go products ship from the factory fully secure. There are no security default values that require modifications by the user to meet PCI security requirements, except the "Bluetooth LE passkey." MagTek recommends one of two options:

1. Devices are ordered with the default passkey changed by MagTek during device configuration prior to shipping
2. The customer change the default passkey with a software utility that changes **Property 1.2.2.3.1.9 Bluetooth LE Passkey** described in ***D998200597 DynaFlex II Go Programmer's Manual (COMMANDS)***.

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 flashing green LEDs 1,3, and 4 as depicted in **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 II Go 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 USB or Bluetooth LE 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 II Go 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
- RSA
- 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 - DynaFlex II Go 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
EMV CA Public keys	Varies per issuer	RSA	Authenticate card data and keys

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:

- ***D998200595 DynaFlex II Go Installation and Operation Manual***
- ***D998200597 DynaFlex II Go Programmer's Manual (COMMANDS)***
- ***D998200593 DynaFlex II Go Device Inspection Document***
- ***D998200594 DynaFlex II Go Package Inspection Document***
- ***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***