

# DynaPro Go

**Secure PIN Entry Device**  
**PCI PTS POI Security Policy**



May 2021

Document Number:  
D998200217-42

REGISTERED TO ISO 9001:2015

Copyright © 2006 - 2021 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.  
DynaPro™ and DynaPro Mini™, are trademarks of MagTek, Inc.  
IPAD® is a registered 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.  
The *Bluetooth*® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by MagTek is under license.

Google Play™ store and Android™ platform are trademarks of Google Inc.

Apple Pay®, OS X®, iPod touch®, iPhone®, iPod®, and Mac® are registered trademarks of Apple Inc., registered in the U.S. and other countries. App Store<sup>SM</sup> is a service mark of Apple Inc., registered in the U.S. and other countries. iPad™ and iPad mini™ are trademarks of Apple, Inc. IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used by Apple Inc. under license.

Microsoft®, Windows® and .NET® are registered trademarks of Microsoft Corporation.

Some device icons courtesy of <https://icons8.com/>, used under the Creative Commons Attribution-NoDerivs 3.0 license.

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

**Table 0-1 - Revisions**

| <b>Rev Number</b> | <b>Date</b>  | <b>Notes</b>  |
|-------------------|--------------|---|
| 10                | Sep 21, 2017 | Initial Revision (Not Released)   |
| 11                | Sep 27, 2017 | Add further details on firmware update procedure  |
| 20                | Apr 4, 2018  | Update for product delta adding 802.11 wireless   |
| 30                | May 31, 2018 | Add supporting information about TLS to section <b>2.5</b> (cipher suites), section <b>3.3</b> , section <b>6.3</b> , section <b>7</b> ; Section <b>3.1</b> clarify wildcard in PCI listings; Section <b>6.2</b> add ECC; Section <b>2.2</b> show all possible hardware IDs; Misc. clarifications and corrections |
| 40                | Jan 8, 2019  | Section <b>4.2</b> align temperatures with latest installation and operation manual; Update for product delta adding Bluetooth Low Energy 4.2; Misc. clarifications and corrections   |
| 41                | Oct 8, 2019  | <b>2.3</b> Add new firmware screenshots with latest revision as a result of a PCI Delta; Misc. clarifications and corrections.  |
| 42                | May 5, 2021  | <b>2.3</b> Add new firmware screenshots with latest revisions as a result of a PCI Delta.   |

## Table of Contents

|   |    |
|---|----|
| Table of Contents .....   | 4  |
| 1 Purpose of This Document .....                                    | 5  |
| 2 General Description .....   | 6  |
| 2.1 Product Name and Appearance .....                               | 6  |
| 2.2 Product Identification .....                                    | 7  |
| 2.3 Firmware Version .....  | 9  |
| 2.4 Application Version .....                                       | 9  |
| 2.5 Communications .....  | 10 |
| 3 Product Guidance .....  | 11 |
| 3.1 Initial and Periodic Security Inspections and Maintenance ..... | 11 |
| 3.2 Configuration Settings .....                                    | 12 |
| 3.3 Default Values .....  | 12 |
| 3.4 Removal from Service .....                                      | 12 |
| 3.5 Servicing .....   | 12 |
| 4 Product Hardware Security .....                                   | 13 |
| 4.1 Tamper Response .....   | 13 |
| 4.2 Environmental Conditions .....                                  | 13 |
| 4.3 Environmental Sensors .....                                     | 13 |
| 5 Product Software Security .....                                   | 14 |
| 5.1 Account Data Protection .....                                   | 14 |
| 5.2 Signing Mechanisms .....  | 14 |
| 5.3 Self-Test .....   | 14 |
| 5.4 Firmware Updates .....  | 14 |
| 6 Key Management .....  | 15 |
| 6.1 Key Management Methods .....                                    | 15 |
| 6.2 Cryptographic Algorithms .....                                  | 15 |
| 6.3 Key Table .....   | 15 |
| 6.4 Key Loading Method .....  | 15 |
| 6.5 Key Replacement .....   | 15 |
| 7 Certificate Management .....                                      | 15 |
| 8 PIN Confidentiality .....   | 16 |
| 9 Roles and Services .....  | 16 |
| Appendix A Reference Documents .....                                | 17 |

## 1 Purpose of This Document

This security policy defines how to properly use MagTek's DynaPro Go product in a secure manner.

DynaPro Go is certified under PCI PTS 4.x, and must be used in accordance with this documentation; any deviation from the approved use of the device described in this security policy will invalidate the device's PCI PTS POI approval.

## 2 General Description

### 2.1 Product Name and Appearance

**DynaPro Go**, shown below, is only to be used as a handheld terminal in attended environments. It is certified as a PCI PTS 4.X PED.

DynaPro Go features include a physical keypad, color display with signature capture, USB, 802.11 wireless and Bluetooth Low Energy communications, magnetic stripe Reader (MSR), contact chip card reader (ICCR), and NFC contactless reader (CTLS).

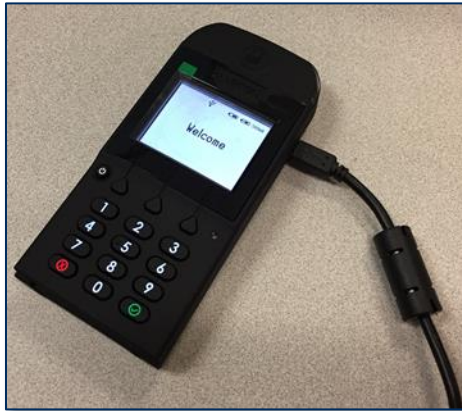


Figure 2-2-1 - DynaPro Go



Figure 2-2-2 - DynaPro Go Front and Back

## 2.2 Product Identification

The device has a label on the back cover, shown in the following figures, which shows:

- 1) Product name
- 2) Device Serial number
- 3) PCI hardware number (“HW”)
- 4) Other supporting information

Do not obscure or modify the label.



Figure 2-3 - DynaPro Go with 802.11 Wireless Device Labels



Figure 2-4 - DynaPro Go USB Only Device Label



Figure 2-5 - DynaPro Go with Bluetooth LE Device Labels



### 2.3 Firmware Version

DynaPro Go provides a **Firmware Version** screen that shows the part numbers and revision numbers of firmware installed on the device. To access this screen, press **Left Function Key** **7** **8** **2** **Right Function Key**. See Figure 2-2-7.

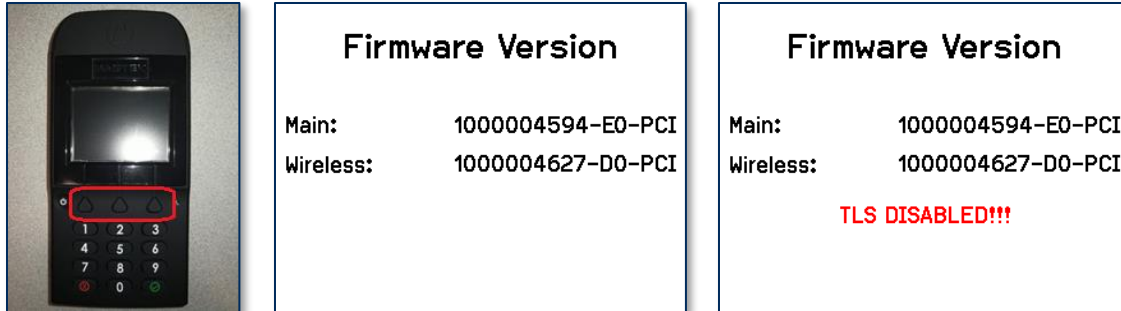


Figure 2-6 - Firmware Version Screen for 802.11 Wireless Devices

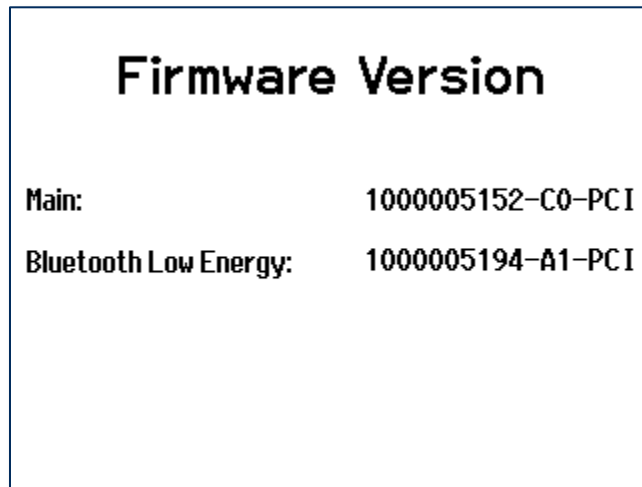


Figure 2-2-7 - Firmware Version Screen for Bluetooth LE Devices

### 2.4 Application Version

DynaPro Go does not support applications of any type.

## 2.5 Communications

The list of host connection types and protocols the device supports are shown in **Table 2-1**. Use of any method not listed in this security policy will invalidate the device’s PCI PTS approval.

**Table 2-1 - Connection Types and Protocols**

| Connection Type          | Protocols   | Available Functions   |
|--------------------------|---|---|
| USB                      | USB HID   | Local updates, configuration<br>Normal operating mode functions |
| 802.11 Wireless b/g/n    | ARP, RARP, TCP, IGMP, IPv4, UDP, ICMP, DHCP Client, TLSv1.2, DNS Client, Gedday DNS Service Discovery | Normal operating mode functions                                 |
| Bluetooth Low Energy 4.2 | SM, ATT, L2CAP  | Normal operating mode functions                                 |

The device supports the following ciphers for secure TLS connections with mutual authentication:

- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

The following Bluetooth Low Energy security features are implemented:

- DynaPro Go implements the Bluetooth Low Energy version 4.2 interface.
- DynaPro Go enforces Security Mode 1 with encryption.
- DynaPro Go enforces Security Level 4, Authenticated Low Energy Secure Connections pairing model with encryption. The Numeric Comparison pairing method is exclusively allowed, Just Works method is neither supported nor allowed.

## 3 Product Guidance

### 3.1 Initial and Periodic Security Inspections and Maintenance

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

- 1) Inspect the label found on the back and make sure the label is not missing, obscured, or modified.
- 2) Check the PCI hardware number on the device label and make sure it matches one of the hardware numbers 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, making sure there are no signs of tampering. Look for unexplained wires or suspicious modifications to the case and keypad area.
- 5) Examine the MSR and Contact reader for any evidence of foreign objects in or near the slots.

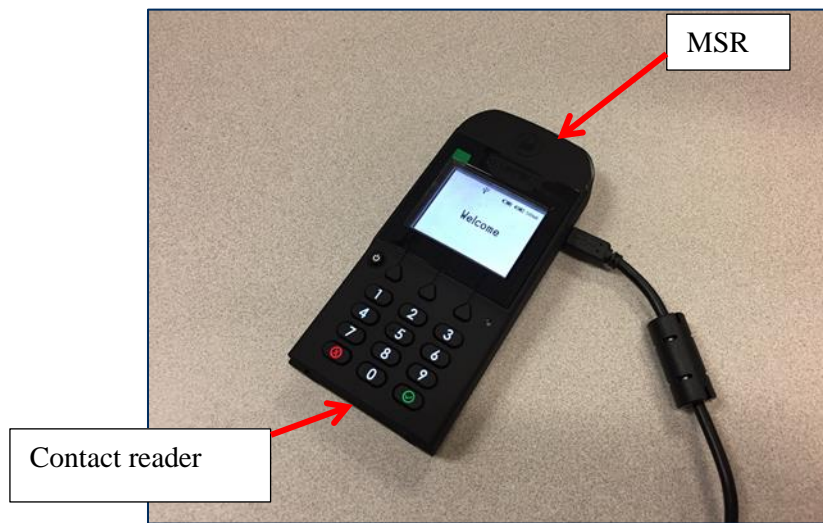


Figure 3-3-1 - MSR and Contact reader

- 6) Power on the Device and make sure **Welcome** appears on the display as shown above.
- 7) Follow the steps in section 2.4 to view the PCI firmware number installed on the device. Make sure this matches one of the firmware numbers listed on the PCI web site for DynaPro Go. Note that in PCI listings, lowercase “x” is a wildcard meaning ‘any single character.’

MagTek strongly recommends performing additional security inspections on a regular schedule. Additional information can be found in **D998200133 DYNAPRO GO DEVICE INSPECTION**. If any problems are detected, stop using the device and contact the manufacturer or your acquirer for further advice.

No periodic maintenance is required for secure operation of the device.

### 3.2 Configuration Settings

DynaPro Go ships from the factory fully secure. The device has no configuration settings that require modification by the user to meet PCI security requirements.

Security-related configuration settings can not be modified by the user. The device only allows configuration changes using current, signed commands from Magensa Remote Services. Contact Magensa for further details.

In addition, non-security configuration settings, such as network addresses and wireless passcodes, can be set up using the **PCIPED\_HASim** tool. This includes the option to enable or disable TLS on models with an 802.11 wireless connection. While this option is useful for initial network setup and testing, **MagTek strongly recommends that TLS always be enabled in the production environment.**

### 3.3 Default Values

There are no security related default values (e.g. passwords) that need to be changed before operating the device. TLS 1.2 network security is enabled by default on models with an 802.11 wireless connection. See the programmer's manual for the device or contact the manufacturer if TLS needs to be disabled (not recommended).

### 3.4 Removal from Service

Before DynaPro Go is removed from service permanently or returned for repair, all the keys and sensitive data must be erased. One way to accomplish this is by temporarily removing the back cover, which will force a tamper response.

If removal of the device 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.

### 3.5 Servicing



**DynaPro Go contains no user serviceable parts inside. Do not attempt to disassemble the device. Doing so will make the unit inoperative, requiring return of the device to the factory.**

## 4 Product Hardware Security

### 4.1 Tamper Response

In the event of a tamper, the device erases all secure keys, blanks the display screen, and goes into a non-operational state. If this occurs, the end user or acquirer should contact the factory help desk. Remove the DynaPro Go from service immediately and store it securely for possible forensics investigation.

### 4.2 Environmental Conditions

The security of the device is not compromised by changing the environmental conditions. Expected environmental conditions for the device are as follows:

- Operating temperature range: 0°C to 45°C (32°F to 113°F)
- Storage temperature range: 0°C to 45°C (32°F to 113°F)

### 4.3 Environmental Sensors



**CAUTION: Operating or storing the device outside the limits described below will cause environmental failure-protection mechanisms to trigger a tamper, causing an erasure of all keys and putting the device into a non-operative state.**

| Sensor                   | Low Threshold Value | High Threshold Value |
|--------------------------|---------------------|----------------------|
| Security Battery (VBatt) | 1.55V               | 2V                   |
| Security Clock           | 14kHz               | 54kHz                |
| Temperature (off)        | -15°C               | 100°C                |
| Temperature (on)         | -20°C               | 100°C                |

## 5 Product Software Security

### 5.1 Account Data Protection

The device supports account data protection using TDEA-CBC encryption. The key being used is the current SRED key based on the DUKPT algorithm. The pass-through of clear-text account data is supported by this device using the whitelisting technique.

### 5.2 Signing Mechanisms

The device will only allow firmware to be installed and executed if it is properly signed. Signature verification is done using RSASSA-PKCS1V15 SHA256 with the 2048 bit RSA Firmware Authentication key.

### 5.3 Self-Test

DynaPro Go automatically performs self-tests at power-up and periodically during the day. The device will also trigger a self-test by resetting itself after no more than 23 hours of continuous operation. No manual operations are required to trigger these self-tests.

Self-tests include:

- Verification of the integrity and authenticity of the firmware.
- Verification that all security mechanisms are enabled and operational.
- Verification of the integrity of all keys

### 5.4 Firmware Updates

DynaPro Go supports file-based updates of the device main firmware, the 802.11 wireless module firmware and Bluetooth Low Energy module firmware.

Firmware updates are provided as files that have been signed by MagTek. The firmware files can be loaded locally over USB by using the MagTek update tool running on a Windows PC. 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 update tool. In addition, the device will indicate failure on the LCD display by showing **Update failed**.

For optimal device security, MagTek recommends the latest versions of firmware should always be installed.

## 6 Key Management

### 6.1 Key Management Methods

The device implements original TDEA DUKPT as its only key management method. DUKPT derives a new unique key for every transaction. For more details, see *ANS X9.24 Part 1:2009*.

### 6.2 Cryptographic Algorithms

The device includes the following algorithms:

- Triple DES (112 bits)
- AES (128 bits)
- RSA (2048 bits)
- ECC (256 bits)
- SHA-256

### 6.3 Key Table

Table 6-1 - DynaPro Go Keys

| Key Name                    | Size      | Algorithm               | Purpose                                      |
|-----------------------------|-----------|-------------------------|--|
| PIN Key                     | 16 bytes  | TDEA DUKPT (ANS X9.24)  | Encrypt PIN block                            |
| SRED Key                    | 16 bytes  | TDEA DUKPT (ANS X9.24)  | Encrypt and MAC Acct Data per X9.24 variants |
| Firmware Authentication Key | 256 bytes | RSASSA-PKCS1V15 SHA-256 | Authenticates firmware updates               |
| Device TLS RSA Cert Key     | 256 bytes | TLS 1.2                 | Support TLS RSA Ciphers                      |
| Device TLS ECC Cert Key     | 64 bytes  | TLS 1.2                 | Support TLS ECC Ciphers                      |
| Host TLS CA Certificate     | Differs   | TLS 1.2                 | Authorize Host TLS Certs                     |

### 6.4 Key Loading Method

The device does not support manual cryptographic key entry. Only specialized tools, compliant with key management requirements and cryptographic methods, can be used for key loading.

### 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 Certificate Management

A trusted Host TLS CA certificate must be loaded into the device before TLS 1.2 can be used for securing network connections. Host certificates are authenticated by the device using the Host CA certificate as part of the establishing a TLS link. See the device's *Installation and Operation Manual* for details. There are no other certificates that can be managed by the customer.

## 8 PIN Confidentiality

DynaPro Go is a hand-held PIN Entry Device used in an attended environment and has no privacy shield. Customers should be advised to protect their PINs by holding the device close to their bodies, shielding the keypad from view.

## 9 Roles and Services

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



## Appendix A Reference Documents

The following documents may be used to provide additional details about the device and this security policy:

- *D998200129 DynaPro Go Installation and Operation Manual*
- *D998200136 DynaPro Go Programmer's Manual (COMMANDS)*
- *D998200133 DynaPro Go Device Inspection*
- *D998200134 DynaPro Go Package Inspection*
- *D998200135 DynaPro Go Quick Installation Guide*
- *NIST SP 800-57-1 Recommendation for Key Management*
- *ANS X9.24 Part 1:2009, Retail Financial Services Symmetric Key Management, Part 1: Using Symmetric Techniques*
- *ANS X9.24 Part 2:2006, Retail Financial Services Symmetric Key Management, Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys*
- *X9 TR-31:2010, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms*
- *ISO 9564-1, Financial Services Personal Identification Number (PIN) Management and Security Part 1: Basic Principles and Requirements for PINs in Card-Based Systems*
- *ISO 9564-2, Banking, Personal Identification Number Management and Security Part 2: Approved Algorithms for PIN Encipherment*