DynaGlass

Payment Terminal
PCI PTS POI Security Policy

June 2021

Document Number:
D998200455-10

REGISTERED TO ISO 9001:2015

MagTek I 1710 Apollo Court I Seal Beach, CA 90740 I Phone: (562) 546-6400 I Technical Support: (888) 624-8350
www.magtek.com

MagTek®, MagnePrint®, and MagneSafe® are registered trademarks 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.
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.
UL™ and the UL logo are trademarks of UL LLC.
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.
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, Google Wallet™ payment service, and Android™ platform are trademarks of Google Inc.
Apple Pay®, iPhone®, iPod®, Mac®, and OS X® are registered trademarks of Apple Inc., registered in the U.S. and other countries. iPad™ is a trademark of Apple. Inc. App Store^{SM} is a service mark of Apple Inc., registered in the U.S. and other countries. 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.

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

Table 0-1 - Revisions

Rev Number	Date	Notes
10	Jun 10, 2021	Initial Release

Table of Contents

Table of Contents 4

1 Purpose 5

2 General Description 6

2.1 Product Name and Appearance 6

2.2 Product Type 8

2.3 Identification 9

2.3.1 Hardware Identification 9

2.3.2 Firmware Identification 10

3 Installation and User Guidance 11

3.1 Initial Inspection 11

3.2 Installation 11

3.3 Environmental Conditions 12

3.4 Communications and Security Protocols 13

3.5 Configuration Settings 13

4 Operation and Maintenance 14

4.1 Periodic Inspection 14

4.1.1 How to Inspect the ICC Card Insertion Slot 14

4.1.2 How to Inspect the Magnetic Stripe Reader 14

4.2 Self-Test 15

4.3 Roles and Responsibilities 15

4.4 Tamper Response 16

4.5 Patching and Updating 16

4.6 Decommissioning 16

4.7 PIN Entry Privacy Message 17

5 Security 18

5.1 Account-Data Protection 18

5.2 Algorithms Supported 18

5.3 Key Management 18

5.4 Key Table 19

5.5 Key Loading 20

5.6 Key Replacement 20

5.7 Key Removal 20

5.8 Signature 20

5.9 Open Protocols 20

6 Software Development Guidance 21

7 Acronyms 21

1 Purpose

This document addresses the proper use of **DynaGlass** devices in a secure manner. This includes information about key management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements.

DynaGlass is a Point of Interaction (POI) allowing merchants to accept banking cards for processing transactions. It is equipped with three card readers: A 3-track magnetic stripe card reader, a contact chip card reader, a contactless card / electronic device reader, and PIN entry capabilities. DynaGlass supports Bluetooth, Bluetooth Low Energy, 802.11 Wireless LAN (WLAN), and USB communication interfaces.

The device is approved as a PTS product under PCI PTS 5.1 requirements. The use of the device in any method not described in this security policy will invalidate the PCI PTS v5.1 approval of the device.

2 General Description

2.1 Product Name and Appearance

DynaGlass looks like **Figure 2-1 below** and **Figure 2-2 below**.

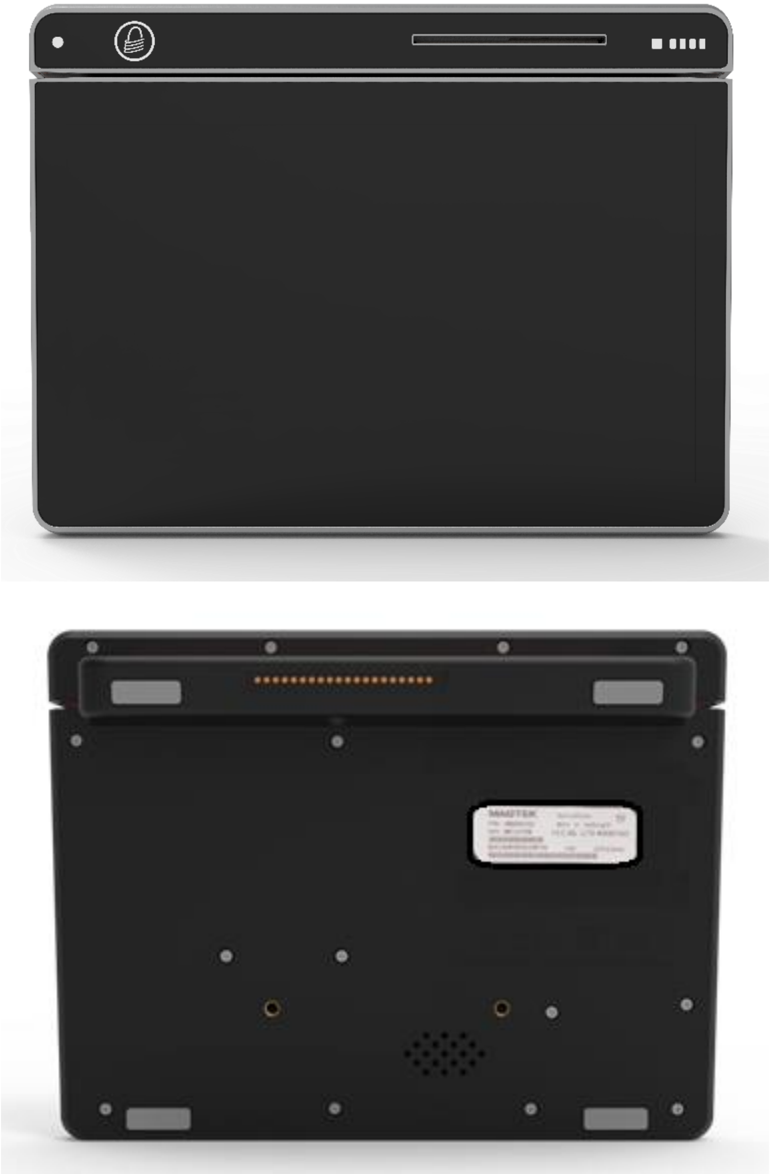


Figure 2-1 - DynaGlass Top, DynaGlass Bottom

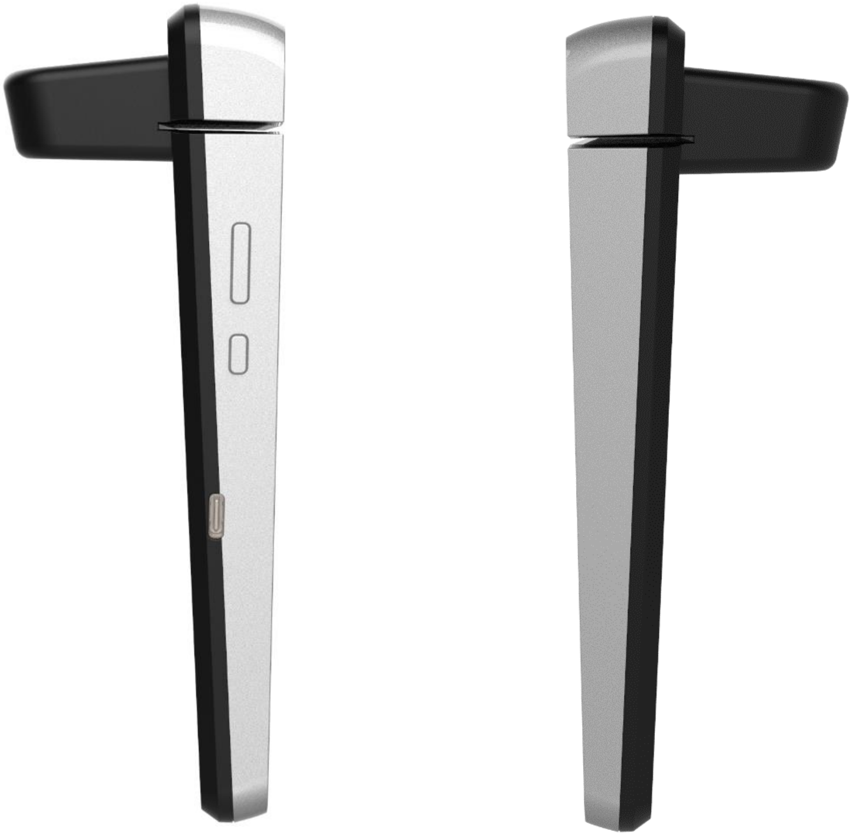


Figure 2-2 - DynaGlass Left Side, DynaGlass Right Side

2.2 Product Type

Approval class: PIN Entry Device (PED) under version 5.1 of the PCI PTS security standard.
Attended or unattended: Attended device.
Handheld or desk-mounted: Desk-mounted.

DynaGlass includes USB communications, a magnetic stripe reader (MSR), a contact chip card reader (ICCR), and a contactless card and electronic device reader (CTLS). It also includes an LCD touchscreen display with PIN entry capability. It is intended to be used as an attended desktop device.

This device is approved as a Point Of Interaction (POI) device under PCI PTS 5.1 requirements, for use in attended environments as follows:

- Card or Proximity Payment Device is present.
- Cardholder is present.
- Cardholder completes the transaction or, if required, an individual representing the Merchant or Acquirer assists the Cardholder in completing the transaction.

Usage in any other manner / environment will invalidate the PTS approval of the device.

2.3 Identification

2.3.1 Hardware Identification

To find important product identification, look on the printed product label on the bottom of the device as shown in **Figure 2-3 below**.

NOTICE

Do not remove, alter, or cover this label.

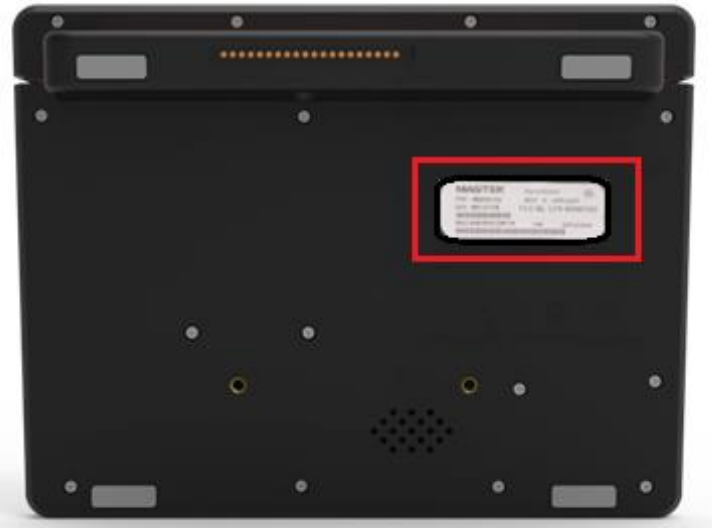


Figure 2-3 - DynaGlass Device Label Location

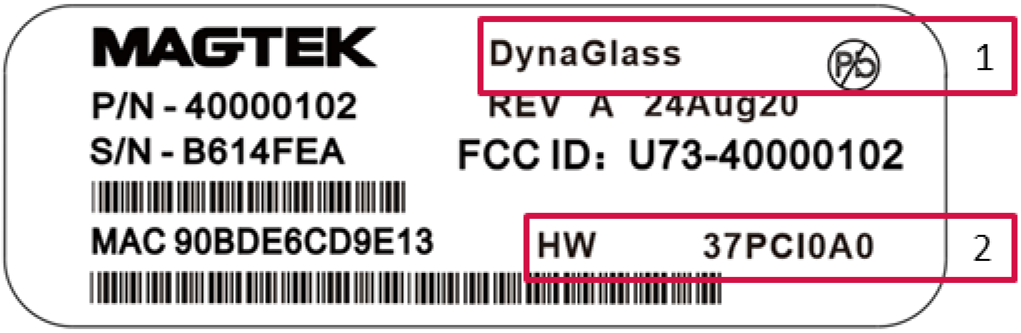


Figure 2-4 - DynaGlass Device Label Contents

The device label includes the following elements of device identification information, shown by the numbered callouts in **Figure 2-4 above**:

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

2.3.2 Firmware Identification

Table 2-1 - Software Version List

Software Item	Version
SP Bootloader Version	1000007851-Ax.xx-PCI
SP Firmware Version	1000007850-Ax.xx-PCI
AP Bootloader Version	1000007853-Ax.xx-PCI
AP System Version	1000007852-Ax.xx-PCI

Each lowercase “x” indicates minor non-security related changes. Users should check to make sure the firmware versions are consistent with vendor provided information (from mail or vendor website).

To view firmware version information, follow these steps:

1) Power on DynaGlass. The device opens to the Android home page, which shows available applications for launch.
2) Launch the **Settings** app, open **About device** section, and scroll down to **FW**.

3 Installation and User Guidance

3.1 Initial Inspection

After receiving DynaGlass, the merchant should visually inspect the device 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 one of the **Hardware #** listed for the device on the PCI web site for Approved PIN Transaction Security (PTS) Devices.
3) Check the device serial number (S/N) and make sure it matches the labels on shipping materials and documentation.
4) Visually inspect the device, per ***D998200442 DYNAGLASS DEVICE INSPECTION***, which is included in the package with the device.
5) Power on the device and make sure it shows the Android home screen, which indicates it is fully powered on and has not detected attempts to tamper.
6) Follow the steps in section **2.3.2** to view the PCI firmware versions installed on the device. Make sure these match one of the **Firmware #** values listed on the PCI web site for DynaGlass. Note that in PCI listings, lowercase “x” is a wildcard meaning ‘any single character.’

3.2 Installation

Connect the device to the dedicated charger and cable included with the device, in an attended environment. The device should be placed away from sources of heat, moisture, dust, and electromagnetic radiation (e.g. display screens, motors, security tag mechanisms, and so on).

3.3 Environmental Conditions

The environmental conditions for the device to operate normally are specified in ***D998200439 DynaGlass Installation and Operation Manual***, available from MagTek. The table below summarizes those conditions:

Parameter	Value
DC Power	5V, 1A
Operating Temperature	0℃ to 50℃
Storage Temperature	-10℃ to 60℃
Humidity	10% < RH <90% (40℃)

The security of the device is not compromised by altering the environmental conditions outside the stated operating ranges above. However, 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 manufacturer for inspection before this condition can be cleared.

Parameter	Value
Secure temperature	-60℃ to 120℃
Secure operating voltage	2.1V to 3.8V

3.4 Communications and Security Protocols

Configuration	Function
Local communication	USB 2.0
Wireless communication	802.11 Wireless LAN (WLAN) Bluetooth (BR / EDR and Bluetooth Low Energy)

Communication methods: USB, 802.11 Wireless LAN (WLAN), Bluetooth.
Communication protocols: TLS v1.2, USB protocol, DHCP, ICMP, ARP, TCP, UDP, IP.
Physical interface functions and data: The USB-C interface is used to transfer non-sensitive data and communications.

Use of any method not listed in this security policy will invalidate the device's PCI PTS approval.

3.5 Configuration Settings

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

4 Operation and Maintenance

4.1 Periodic Inspection

Because the device handles confidential data such as cardholder PIN codes, the merchant or acquirer should check the device at least once per week for any suspicious alterations, such as:

- Missing screws
- Suspicious wires connected to any ports
- Hardware and software versions on the device label or display that are not consistent with listed / approved versions
- Missing tamper seal
- Housing damage
- Additional stickers or labels
- Suspicious items around IC and MSR reader. See pictures in section **2.1** and ***D998200442 DYNAGLASS DEVICE INSPECTION***, available from MagTek and included with the device.
- Incorrect or redundant overlays on the touchscreen display
- Failures when device self-test runs at 00h:00m daily, as described in section **4.2**

If you find anything suspicious and are not sure whether it is a security risk, contact your vendor representative for assistance.

In the tampered state, device removes all keys saved in its Secure Processor, shows a notification message, and locks the device, making further use of the device impossible. If you observe a tamper notification message, contact your representative for assistance.

4.1.1 How to Inspect the ICC Card Insertion Slot

To make sure the ICC card interface is secure, the merchant should check for the following. If any of these conditions occur, immediately take the device out of service and contact your vendor representative for security inspection. For a reference showing what the ICC card interface should look like, see DynaGlass Top in **Figure 2-1** on page **6**.

- Suspicious wires around the card insertion slot.
- ICC cards can not be inserted smoothly. The insertion should feel smooth and unobstructed.
- Damage or alterations to the housing of the ICC interface.

4.1.2 How to Inspect the Magnetic Stripe Reader

To make sure the magnetic stripe reader (MSR) is secure, the merchant should check for the following. If any of these conditions occur, immediately take the device out of service and contact your vendor representative for security inspection:

- Any additions in or around the MSR swipe path, including suspicious wires.
- MSR swipe path guide has been damaged or destroyed.
- Cards can not be swiped smoothly. The swipe path should feel smooth and unobstructed.

4.2 Self-Test

The device automatically performs self-tests during power on and reset. To reinitialize memory, the device reboots whenever its internal real-time clock reaches 00h:00m. Self-tests are not initiated by an operator. The self-tests include:

- Firmware integrity and authenticity
- Hardware security status check

If the self-tests detect any kind of failure, the device shows a prompt indicating the tamper status. If this occurs, the device is disabled and can not be used for transactions. Contact an authorized service center to arrange for repairs.

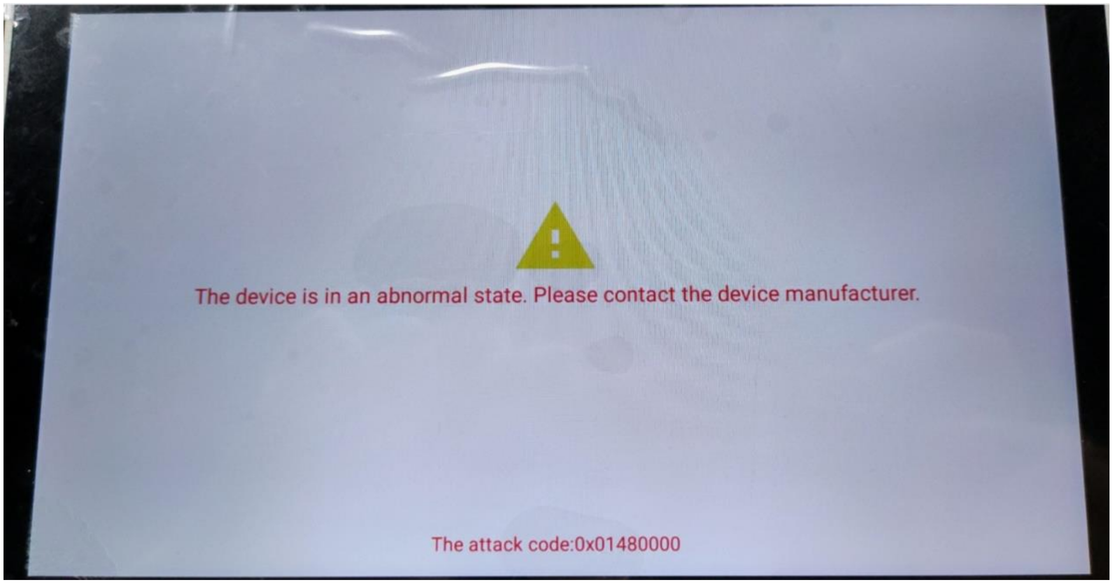
4.3 Roles and Responsibilities

MagTek generally sells directly to merchants, or indirectly to merchants via Value Added Resellers (VARs) and acquirers. MagTek provides technical support and maintenance to its direct customers, while the acquirers and VARs provide support to their merchant customers. MagTek, VARs/acquirers, and merchant end users play different roles in operating the device:

Participant	Role	Responsibilities
VAR/Acquirer/Merchant	Administrator	Organize third parties to develop solution designs, including applications that run on the device
Merchant / End user	Operator	Perform transactions
MagTek	Maintainer	• Support and maintain devices • Repair devices and unlock devices if tampered • Sign customer public keys, load customer public keys and applications into the device

4.4 Tamper Response

In the event of a tamper response, the device erases all keys from its Secure Processor, enters a disabled state, and shows a locked down tamper detection message. The device's buzzer beeps based on the nature of the tamper condition. After this occurs, no other prompts are available, and operators can not perform any further secured functions. If this occurs, contact your representative for assistance.



The device is in an abnormal state. Please contact the device manufacturer.

The attack code:0x01480000

4.5 Patching and Updating

DynaGlass supports file-based updates of the device's firmware and applications. Firmware updates are provided as files that have been signed by MagTek. The firmware files can be loaded locally via the device's USB port using the MagTek update tool running on a Windows PC. The firmware files can also be loaded via a secure remote updating process using Open Protocol HTTPS with TLS1.2.

The device verifies that 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 optimal device security, MagTek recommends installing the latest versions of firmware at all times.

Note that updates to security-related prompts, such as prompts to enter or re-enter a PIN, are not considered minor changes and require the firmware version to be updated (see section **2.3.2 Firmware Identification**).

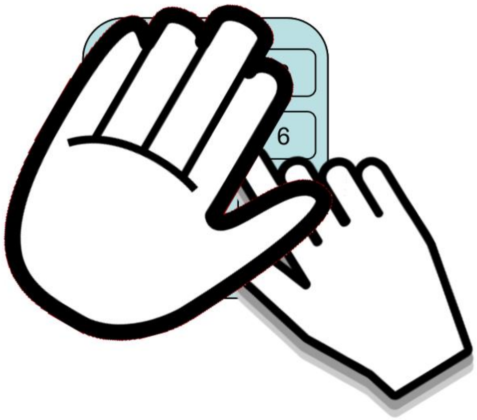
4.6 Decommissioning

To permanently decommission the device or to otherwise clear all encryption keys and sensitive data from device memory, follow these steps:

1) Locate the long rectangular panel on the back of the device that has only three screws installed.
2) Completely remove all three screws.
3) Make sure the device reports it has detected a tamper event (see section **4.4 Tamper Response**).

4.7 PIN Entry Privacy Message

Because DynaGlass supports PIN entry and does not provide an integrated privacy shield, merchants must provide cardholders with the necessary privacy and guidance to enter PINs safely and securely. One method is to include guidance messages and logos for the cardholder as part of the payment application. The figure below shows an example of a safe PIN entry logo which could be displayed by the application prior to, or in conjunction with, the PIN entry prompt message. Such messages and graphics must convey easy-to-understand information about how to protect the PIN from sight, such as by using the cardholder's own body or their free hand to block the view of the keypad.



In addition, position the device in a way that makes cardholder PIN spying infeasible. Attendants should be trained to assist cardholders in ensuring that others are not looking while they are entering their PINs.

The following table shows the combinations of PIN privacy methods that must be put in place when installing the device to protect the cardholder's PIN during PIN entry.

Method	Observation Corridors				
	Cashier	Customer Queue	Customer Elsewhere	On-Site Cameras	Remote Cameras
Fixed Desktop	Position device facing away from the cashier. Use signage to block cashier's view. Back to the crowd	Position device facing away from the cashier. Use signage to block cashier's view. Back to the crowd	Position device facing away from the cashier. Use signage to block cashier's view. Back to the crowd	Do not install within view of cameras	Do not install within view of cameras
Mobile Scenario	Position device facing away from the cashier. Use signage to block cashier's view. Back to the crowd	Position device facing away from the cashier. Use signage to block cashier's view. Back to the crowd	Position device facing away from the cashier. Use signage to block cashier's view. Back to the crowd	Do not install within view of cameras	Do not install within view of cameras

5 Security

5.1 Account-Data Protection

The device always encrypts account data from all three readers using an ***X9.24 DUKPT*** derived data key. The device does not support any mechanisms, such as whitelists or SRED disable settings, that would allow account data to be transmitted unencrypted.

5.2 Algorithms Supported

The device includes the following algorithms:

- Triple DES (128 bits)
- AES (128 bits, 256 bits)
- RSA (Signature verification, 2048 bits)
- SHA256 (Signature digest)
- ECC (P-256, P-384, P-521)

5.3 Key Management

The device supports the DUKPT key management method. This method uses a unique key for each transaction, and prevents the disclosure of any past key used by the transaction-originating device.

Using any other key management methods will violate the PCI PTS approval of the device.

It is forbidden to load same key to multiple devices. Each device must have unique keys.

5.4 Key Table

The transaction related keys are classified as follows. The algorithms used by these are TDES and AES. These transaction keys (except Future DUKPT Keys) are controlled by the acquirer. None of the keys loaded into the device can be obtained from the device in any way. These keys can only be used for their intended purposes via the interfaces or commands provided by the device.

Key Name	Purpose/Usage	Algorithm(s)	Size(Bits)
SKEK	Encryption of working keys downloaded into the device and saved in Flash	AES	256
Transport Keys	Key injection	AES TR-31 KBPKs	256
MAC Key	MAC Encipherment	AES	128, 256
Account Data Key	Account Data Encipherment	TDEA DUKPT (ANS X9.24-3)	128
PIN Key	PIN Block Encipherment (Format 0/1/3)	TDEA DUKPT (ANS X9.24-3), ANS X9.8-1/ISO 9564-1	128
PIN Key	PIN Block Encipherment (Format 4)	AES DUKPT (ANS X9.24-3), ANS X9.8-1/ISO 9564-1	128, 256

5.5 Key Loading

The device does not support manual cryptographic key entry. Only a specialized Key Loading Device, compliant with key management requirements and cryptographic methods, specifically ***TR-31***, can be used for key loading. Use of any other methods will invalidate PCI approval.

5.6 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***. If a tamper event has occurred, the device must be returned to MagTek for security inspection and secure re-injection of new keys.

5.7 Key Removal

After keys are successfully injected into the device, there are two ways to remove them:

- Passively erasing keys, performed by firmware or hardware, such as when a tamper event occurs.
- Actively erasing keys, performed by an authorized user with a dedicated software tool, for example during manufacturer repair or decommissioning.

5.8 Signature

The device uses asymmetric cryptographic algorithms for software signature verification:

- SHA256 and RSA 2048 are used for Application Processor (AP) firmware signature verification.
- SHA256 and ECDSA-P256 are used for Secure Processor (SP) firmware signature verification.
- SHA256 and ECDSA-P384 are used for Application Processor (AP) application signature verification.

The signing keys are controlled only by MagTek. Software authentication is performed within the device by signature verification using the corresponding public key.

5.9 Open Protocols

The following describes the communication methods and protocols available in the device:

	Interface	Protocols
Communication	802.11 Wireless LAN (WLAN)	TLS, IP, TCP, UDP, ARP, DHCP, ICMP
	Bluetooth	SMP, GATT, ATT, L2CAP, HCI, LL

Data transferred between the device and remote hosts via the 802.11 Wireless LAN (WLAN) connection is encrypted with security protocol ***TLS1.2***. Application developers can use TLS by calling a library available on the device. During the TLS connection phase, the private key of the device is needed. The private key is pre-embedded in the Application Processor's firmware.

The device also supports Bluetooth 4.2 protocol for Bluetooth secure communication. In Bluetooth Low Energy mode, the device uses low energy security mode 1 level 4. The Bluetooth "Just Works" pairing mode is disabled.

Support version: openssl-1.0.2g TLSv1.2
SSL has inherent vulnerabilities. DynaGlass does not support SSL.

6 Software Development Guidance

Developers of custom applications must follow the guidance for application development, validation and deployment as detailed in the "Software API Development Guide" document reference. Following the recommended process and using the provided APIs ensures the application will be compliant with PCI-PTS security requirements.

7 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AP	Application Processor, the processor in the device that runs the Android operating system and installed applications
DUKPT	Derived Unique Key Per Transaction
PED	PIN Entry Device
PIN	Personal Identification Number
RSA	Rivest Shamir Adelman Algorithm
SHA	Secure Hash Algorithm
SP	Secure Processor, the processor in the device that controls the device's embedded reader hardware
TDES	Triple Data Encryption Standard
VAR	Value Added Reseller

Appendix A References

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

1) ***Software API Development Guide***
2) ***D998200439 DynaGlass Installation and Operation Manual***
3) ***D998200442 DynaGlass Device Inspection***