PCI Scope, Compliance, and Risk Assessment
for MagTek Secure Card Reader Authenticators (SCRAs)

The purpose of this document is to help users of MagTek devices to formulate their own methods and procedures for device inspection and security for their MagTek Secure Card Reader Authenticator devices when in use. The following provides best practices and recommendations to simplify your device inspection and assessment.

Best Practices

Use MagTek SCRA Devices

SCRA devices deliver enhanced security and exceed industry standard compliance and security measures. SCRA devices use engineering design best practices to help prevent physical attack and use the MagneSafe® Security Architecture to prevent logical attack. MagneSafe provides a digital identification and authentication architecture that safeguards consumers and their personal data. MagneSafe leverages: strong TDEA encryption using the DUKPT key management scheme; the secure tokenization of data in Magensa Gateway services; counterfeit detection of cards, devices and data; tamper recognition; and dynamic digital transaction signatures; which together validate and protect the entire transaction and each of its components.

Inspect and Verify Devices are Valid

Inspect your installed and stored SCRA devices regularly and match their serial numbers (electronic serial numbers when applicable) to inventory lists whenever possible. Keeping a secure inventory of device functionality, serial numbers, reserved devices, replaced devices, and repaired devices helps prevent rogue devices from entering your environment. Inspecting cable connection can also determine if rogue devices, or transmitters have been attached to your devices. Also, use good business practices and always verify repair technicians that service any of the system components.

Don't Store Cardholder Data

Don't store cardholder data in your environment. If you have to store data, do not store cardholder data in the clear. Make certain the data is encrypted and secured. MagTek hardware and Magensa Services deliver solutions that help ensure the system under test and cardholder data are secure.

Theft Prevention and Secure Disposal

Track and secure devices so they are not stolen. When devices are not in use, if possible, secure them in an inventory controlled environment with proper security checks.

If devices are brought out of service, ensure they are disposed of following local guidelines for similar materials.

SCRA devices do not store sensitive cardholder data, therefore the device itself is not a liability.

Card Present Transactions

Merchants should swipe all transactions to take advantage of encryption, which helps reduce the scope of PCI, and magnetic stripe authentication, which stops counterfeit cards.

Manually entered transactions typically increase PCI scope and cost more. DynaPAD secures manually entered data by performing encryption to data entered on the keypad and may reduce or remove added costs associated with card not present transactions.

Prevent Physical Attack

Device Inspection

The enclosures for MagTek SCRA devices are tamper evident and the head assembly is tamper resistant. The form factor would need to be broken to access inside the devices and attempts to break into the device would most likely make the device non-operational. On a regular basis perform visual inspection of the devices to ensure there are no signs of tampering. If you see any evidence of tampering report this immediately to your installation provider. Be certain to refer to your particular device's Installation and Operation manual for more comprehensive details.

Form Factor

Confirm overall form factor dimensions and weight. See Comparison Chart for device size and weight. The form factor is a smooth rubberized shell. The seam between parts is very tight. There are no additional electronics or wires. Any breaks in the plastic, scuffs, or damage could be signs of physical tampering and should be reported.

Swipe and Insertion Paths

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 makes contact with the read head. There are no other mechanics, electronics or wires in the swipe path. eDynamo and iDynamo 6 have EMV capability and a card slot for the EMV cards. The card slot is a smooth slot with only the contact head. There are no other mechanics, electronics or wires in the insertion path. iDynamo 6 has contactless reading capability and a clearly indicated tap pad is visible and printed directly to the plastic.

LEDs

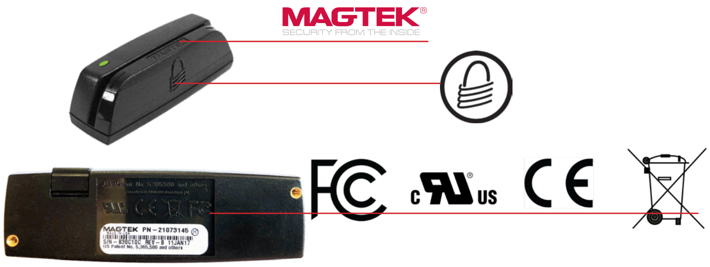
Except the iOS family of devices, SCRA devices have LEDs. The LED indicator(s) reflect the status of the reader. Reference the devices' Quick Installation Guide to ensure the LED behaves as expected.

Connections

See Comparison Chart to ensure the proper connection is being used. Certain models connect via wireless connection, USB or Lightning. USB interface is provided to allow devices to either charge the internal, rechargeable battery and/or interface with iOS, Windows, or OS X based computers which provide a host USB interface. There are no additional wires. Ensure the wire(s) and/or connection looks familiar and has a direct connection to the host.

Movable and Removable Parts

Several readers have movable and/or removable parts. Reference the Comparison Chart to verify these components. These can include mounting brackets, stabilizing clips, stabilizing tape or Velcro®, or mounting screws. No extraneous wires or electronics are used to connect these items other than their selected cables.



Logos and Emblems

There is a de-bossed MagTek logo imprinted directly to the plastic form factor. There is an embossed MagneSafe® Logo lock imprinted directly to the plastic form factor. Certificate logos (CC, UL, CE, Waste Electrical logos and US Patent number) are embossed directly to the plastic form factor or in the Quick Installation Guide.

Product Tag

On the device there is typically a product tag. It lists part number (PN), serial number (S/N), revision (REV), date of production, and a bar code. Ensure that the tag matches the in-house inventory. Ensure an additional label hasn't been over-laid to hide a transmitter or wires.

Keypads

DynaPAD has a keypad. Ensure there are no keypad overlays or unwanted movable parts.

Prevent Logical Attack

Mutual Authentication

Devices can be configured to require mutual authentication with an authentication / cryptographic host before it will transmit card data. This functionality can be activated by the app. SCRA devices use time bound session IDs to prevent replay attacks.

Secure Encryption

MagTek utilizes open standards Triple DES encryption and DUKPT (derived unique key per transaction) key management to provide a comprehensive security solution that protects cardholder data with dynamic encryption from the earliest point of the transaction. PAN output can be masked to allow verification of the transaction. A partly obfuscated account number, cardholder name and card expiration date can be sent to the host as clear text where they may be displayed, retained, or become part of a receipt.

Card data is encrypted within the SCRA devices prior to being sent to the host. Encrypted data will be sent through the connector to the app, which will then transmit it to a cryptographic host for decryption. The host has no knowledge of the decryption key ensuring that cardholder data is protected.

Tamper Resistant and Evident

SCRA devices are tamper resistant and tamper evident devices. The devices are compliant with ANSI X.9 standards, including encryption of sensitive payment card data and key management. Since the devices use a DUKPT key management methodology (a unique key is automatically generated for every transaction) only one key could possibly be compromised, greatly reducing risk. No past keys or future keys could be deciphered. There is no risk for the BDK to be compromised. eDynamo goes a step further and is tamper responsive; this ensures that breaking into the enclosure will activate the tamper sensor and erase the key.

There are No User Controls

Control, status, and data functions are provided by the host interface. The system requires software on the host device to direct the operation of the card reader through the Application Programming Interface (API).

There is No Opportunity for Malware

The devices are host driven. This gives users the confidence that their customer data cannot be compromised by malicious software on their devices. Malware cannot be uploaded to SCRA devices.

Devices pictured in order from top left of page 2 - iDynamo 6, eDynamo side angle, eDynamo top angle, Dynamag front angle, iDynamo 6 front angle, aDynamo front with audio jack extended and stabilizer clip, Dynamga bottom and side, iDynamo 5 (Gen II) back, DynaPAD side.

Limitations of PCI Compliance
This document in no way guarantees PCI compliance or scope reduction. Ultimately the PCI classification and scope are determined by the merchant's Qualified Security Assessor (QSA).

Comparison Chart

Below is a comparison chart of our secure card reader authenticators (SCRA devices). As part of your inspection, it is recommended to have a list of each device name, product tag information, and its location. It may be helpful to take photos of the front, back, and sides of each device for ongoing comparison.

	Dynamag	DynaPAD	eDynamo	iDynamo 5	iDynamo 6	tDynamo
Payment methods						
Magstripe secure card reader authenticator Triple Track (TK1/2/3); Bidirectional read ISO 7810, 7811; AAMVA driver licenses	YES 4 ips to 60 ips	YES 4 ips to 60 ips	YES 6 ips to 60 ips	YES 4 ips to 60 ips	Yes	YES 4 ips to 60 ips
EMV chip contact EMVCo L1 and L2 ISO/IEC 7816	NA	NA	YES	NA	Yes	YES Terminal type 21 and 24
Contactless (EMV and NFC)	NA	NA	NA	NA	Yes	YES
Reliability and Operation						
MSR / SCRA swipes	1 Million	1 Million	250K	1 Million	200K	200K
EMV insertions	NA	NA	100K	NA	200K	100K
Compatible Host Operating System	Windows plug & play	Windows plug & play	iOS, Android and Window	iOS	iOS, Android and Window	iOS, Android and Window
Status indicators	Status LED (Green)	Status LED (Green)	Wireless Status LED (Blue) Status LED (Red/Green/Amber)	NA	1 LED	4 LEDs
General						
Connection Method	USB Type A plug, 6ft	USB Type A plug, 6ft	Micro-USB B [HID]	Lightning	USB-C Lightning	USB Bluetooth LE
Wireless (Frequency 2.4 MHz)	NA	NA	Certain standard wireless	NA	NA	Bluetooth LE
Interface	USB HID and USB KB	USB HID and USB KB	USB, Wireless	iOS	Lightning and USB	USB Bluetooth LE
Display	NA	2 line by 16 digit liquid crystal display (LCD) Secure 15-key pad	NA	NA	NA	NA
Optional Accessories	NA	NA	Retractable cable Optional docking station	Retractable cable Stabilizers	Battery and stabilizer	Stand uniVERSE Clip
Electrical						
Charging	None	None	Rechargeable Micro-USB charge Charging Time 3Hr	USB charging adapter (Requires port with 2A @ 5V)	Power through iOS or USB. EMV/NFC Contactless requires battery pack	Rechargeable USB 2.0 charge
Battery	No battery	No battery	Li-ion Polymer 800 mAH & Coin cell backup	No Battery	optional	Li-ion Polymer
Current and Power	Power via USB 100 mA max USB: 5V	Power via USB 100 mA max USB: 5V	Power via USB or Battery. USB: 5 VDC | ~ 500mA Battery: 3.7 VDC | > 100 mA	Powered thru iOS device 50 mA current draw 2.85 to 3.47 VDC from device	Li-Po 400mAh	Power via USB or Battery. USB: 5 VDC
Security and Certifications						
Compliance (FCC, CE, UL)	YES	YES	YES	YES	YES	YES
Data protection 3DES encryption; DUKPT key management MagneSafe Security Architecture Unique, non-changeable device serial number	YES	YES	YES	YES	YES	YES
Tamper	Evident/Resistant	NA	Evident/Resistant	Evident/Resistant	Evident/Resistant	Evident/Resistant
Mechanical						
Dimensions L x W x H or L x W x D	3.92 x 1.24 x 1.2 (99.5 x 31.6 x 30.4 mm)	5.90 x 4.00 x 1.51 in. (150 x 102 x 38 mm)	2.45 x 1.52 x 0.97 in. (62.2 x 38.7 x 24.7 mm)	2.47 x 1.5 x 0.58 in. (62.7 x 38.1 x 14.7 mm)	2.75 x 2.1 x 0.73 in. (70 x 53.9 x 18.75 mm) with battery pack: 2.8 x2.24 x 1.3 in. (72.72 x 57.8 x 33.0 mm)	3.94 x 3.25 x .61 in. 100 x 82.5 x 15.5mm
Weight	1.8 oz. (50 gr) without cable	9.3 oz. (263.651 g)	2.2 oz. (60 g)	w/o adapter 1.02 oz. (28.94 g)	iDynamo 6: 0.90 oz. (25.4g) Battery pack: 1.68 oz. (47.6g)	Reader: 3oz (83g) with stand: 10oz (285 g)
Mount/Stabilizer	Screws or fastening tape	Velcro®	Optional docking station	Device adapters	Optional	Stand, Clip
Environmental						
Operating temp	32°F to 158°F (0°C to 70°C)	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)	32°F to 95°F (0°C to 35°C)	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)
Operating and Storage Humidity non-condensing	10% to 90%	5% to 90%	5% to 90%	5% to 90%	5% to 90%	10% to 90%
Storage temp	-40°F to 158°F (-40°C to 70°C)	-4°F to 149°F (-20 °C to 65 °C)	14°F to 140°F (-10°C to 60°C)	-4°F to 113°F (-20°C to 45°C)	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)

MAGTEK®
SECURITY FROM THE INSIDE

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.

Founded in 1972, MagTek is a leading manufacturer of electronic systems for the reliable issuance, reading, transmission and security of cards, barcodes, checks, PINs and identification documents. Leading with innovation and engineering excellence, MagTek is known for quality and dependability. Its products include secure card reader/authenticators, Qwantum secure cards, token generators, EMV contact, contactless, barcode and NFC reading devices, encrypting check scanners, PIN pads and distributed credential personalization systems for secure magstripe and EMV enabled cards. These products are used worldwide by financial institutions, retailers, payment processors, and ISVs to provide secure and efficient data privacy, as well as payment and identification transactions. Today, MagTek continues to innovate. Its MagneSafe® Security Architecture leverages strong encryption, secure tokenization, dynamic card authentication, and device/host validation enabling users to assess the trustworthiness of credentials and terminals used for on-line identification, payment processing, and high-value electronic transactions. MagTek is headquartered in Seal Beach, CA.