MAGTEK®
SECURITY FROM THE INSIDE

iDynamo 5 (Gen III)
Secure Card Reader Authenticator

Device Inspection Document

IMPORTANT: Be certain to inspect this device before deployment and during its life-cycle.

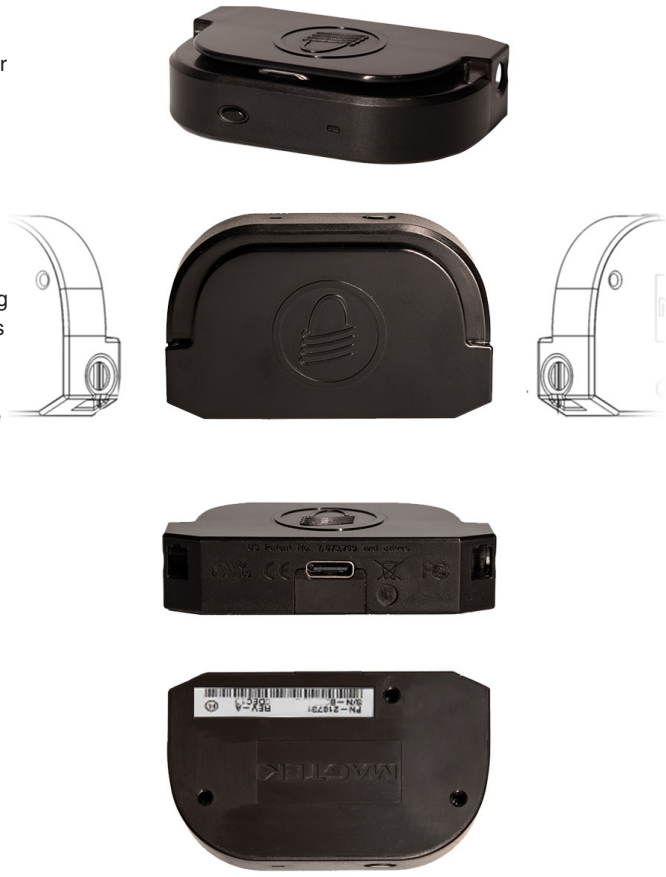
Overview

iDynamo 5 (Gen III) is a compact secure card reader authenticator (SCRA) that reads magnetic stripe cards that conform to ISO standards. iDynamo models are made for iOS, Android, and Windows devices equipped with a USB-C or Lightning interface. When a cardholder swipes a card, the device encrypts card data before they leave the encapsulated magnetic stripe reader head using the Triple Data Encryption Algorithm (TDEA, also known as Triple DES) and DUKPT key management.

Form Factor

The exterior of the device is a a rubberrized plastic. Visually inspect the device for signs of tampering. There should be no evidence of loose wires or screws, misplaced labels, cracked casing, holes, or tool marks.
Front Face: Inspect the overall form factor for signs of tampering. The front face has an embossed MagTek lock.

- **TOP:** The top of the device has a single LED and power button.
- **General Status LED:** Power on the device and make sure that there is no indication that potential tampering was detected. After the device goes through the boot-up process, the LED should be solid green.
- **Bottom:** A single USB-C receptacle is on the bottom of the device with certification and compliance logos as shown in the image.
- **Reader Left:** There are 2 adapter sleeve retainer holes. There are no other components.
- **Reader Right:** There are 2 adapter sleeve retainer holes. There are no other components.
- **Reader Back:** The MagTek logo is debossed into the plastic and the product label in located on the bottom right.
- **Magnetic Swipe Path:** Check the card insert slot. The reader has a smooth, unobstructed path. Insert an embossed card into the device to check for any signs of obstructions inside the card insertion slot. Other than the magnetic head that reads magnetic stripes there are no electronics, objects, or wires in the path.
- **Product Label:** The product label is located on the back of the device. Check PN, SN and HW number. Serial Number matches serial number on boot-up. Check the product label on the device is complete, fully attached, with no signs of modification.Check the information (part #, model name, and serial number) on the label and ensure it matches the information found on the package and in any documents such as invoices.



Shipment

Check shipping documents and tracking information to ensure that the shipment origin and sender information are correct. Check for evidence of tampering with the package containing this device. Before shipment, the box is sealed with tamper evident tape that will show VOID and OPENED if removed. The box and seal should be intact when initially received.

Checklist Summary

Check all views of the device and compare to photos.

Device Audit

It is helpful to do the following for your device inspection audit.

- Have a list of the device sand details listed on the asset tag.
- Take photos of the front, back, and sides of each device.

Check device Part numbers, serial numbers and IDs and check physical connections. Report any suspected signs of tampering immediately.

PCI compliance web page.
How to find on PCI web site https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices.
Search for MagTek and find the product name, oiDynamo 5 (Gen III), on the web page. Compare the Hardware # and Firmware #.

Periodically inspect the following items while in use:

- Card swipe path
- Power Button
- Form factor
- LED
- Label
- USB-C receptacle