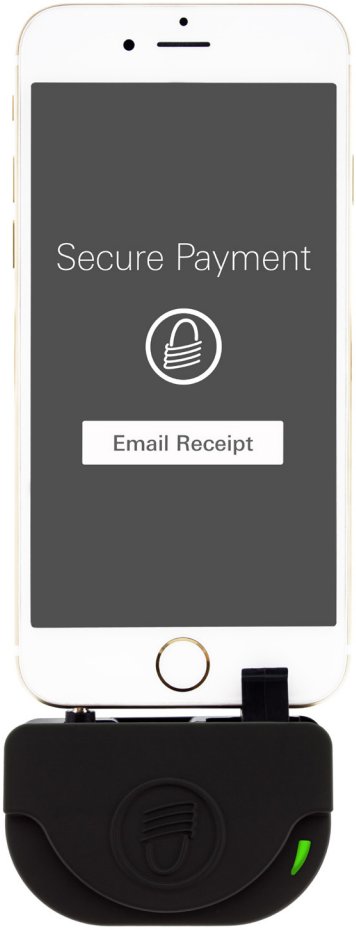
MAGTEK®
SECURITY FROM THE INSIDE



uDynamo
Secure card reader authenticator
connected to mobile device

uDynamo for Retail

Secure Card Reader Authenticator

MagTek's uDynamo provides universal connection options for its users. uDynamo secure card reader authenticator connects to a wide variety of devices (more than 221 mobile phones and tablets as of Feb 2014) through its retractable headphone jack. It also provides a USB interface for connection with various devices including Windows or Mac PCs, and is perfect for use with a virtual terminal.

MagTek's uDynamo is built around the MagneSafe® Security Architecture (MSA), a layered approach to transaction security that combines encryption, tokenization, authentication and dynamic data to protect payment transactions and card data from the point of swipe.

uDynamo combines the latest technologies to be the most secure, versatile, reliable and cost-effective mobile reader in the market.

iOS

Call a representative to learn more: 562-546-6400.

MagTek® Inc., 1710 Apollo Court, Seal Beach, CA 90740 | p 562-546-6400 | f 562-546-6301 | 800-788-6835 | www.magtek.com

uDynamo Design Features

Adjustable stabilizer for a variety of devices

The adjustable stabilizing grips allow uDynamo to easily attach to a wide variety of phones and tablets allowing the user to adjust the fit for optimum mounting stability. The stabilizer grips can be adjusted in 3 different positions with two different size grips, enabling uDynamo to avoid interference with on/off buttons, cameras, protective cases and other design elements that are unique to each phone/tablet.

Swipe path design yields highest read reliability on first pass

The swipe path is designed for maximum stability as the card and mag stripe travels over the read head ensuring a more consistent and reliable card read. Smaller readers might be cute, but they are more difficult to work with and often require more training, significant dexterity and often two hands for swiping and stability. Because of this, users may often find it necessary to swipe cards several times before a good read occurs.

Rechargeable on-board battery allows for 1,000,000 swipes

Lower cost readers have a total life expectancy of 20K swipes. By using a re-chargeable battery, uDynamo can deliver about 1 million lifetime swipes.

Retractable headphone jack interface - digital output

Fixed headphone jacks can easily break, get in the way and even poke you while in your pocket. uDynamo was designed to allow the headphone jack to retract and move out of the way when not in use.

USB interface (power and comm i/o)

UDynamo is the first mobile reader that can also connect to a PC or Mac computer for additional use with a virtual terminal, thus extending its overall value and use cases.

Track 1, 2 and 3 data

UDynamo can read 3 tracks of data capturing alpha and numeric account data. Track 2 only readers cannot read alpha data from ATM/credit/debit/gift cards. By capturing more track data, uDynamo delivers more information that can be used to ensure the card that is swiped has the same embossed and printed account holder data as compared to the encoded data on the stripe. Having access to Track 1 data, users can read account holder name information and address their customers by name as well as have data redundancy in the event there is a read error on either track 1 or 2, but NOT both.

Reads ANSI/ISO/AAMVA cards

UDynamo can also read data that is encoded to national and International standards. This allows uDynamo developers to enhance their applications with value-added identification and read functionality that includes the ability to read many US drivers' licenses.

uDynamo Security

Triple DES encryption sealed inside the head

UDynamo encrypts all the data within the confines of the magnetic head. The encryption of the decoded magnetic wave patterns and the authentication data occurs before it leaves the magnetic head. Hence, any data that can be monitored or trapped along the external head wires has already been encrypted with a unique key, rendering it of no value to a malicious coder. By utilizing encryption inside the read head, criminals have no opportunity to gather clear-text card data prior to encryption taking place. By using Triple DES/3DEA, uDynamo delivers a powerful, fully vetted, open-standard encryption algorithm.

Derived Unique Key per Device and Transaction

By utilizing DUKPT key management, every uDynamo has a unique set of encryption keys that dynamically change with every swipe, making key management easy and robust. The encryption keys are injected using services that have been certified as TR-39 compliant. This helps merchants and their service providers alike by removing significant risks that accompany securing, managing and having access to encryption keys. Competitors that offer DUKPT key management with the AES algorithm are doing so in the absence of national and internationally agreed upon standards. This proprietary key management technique is NOT an open standard.

Remote configuration and key loading

UDynamo can securely accept a remote key injection/device configuration by utilizing web services from MagTek and Magensa, both TR-39 certified and official ESOs. For more details on MagTek and Magensa's PCI-DSS or ESO status, visit VISA's Global Registry of Service Providers. Some competitors provide FREE utilities that can inject encryption keys. These FREE services are NOT certified as TR-39 compliant and can place merchants and their providers at significant risk for PCI DSS non-conformance, and open up opportunities for criminals to build their own encrypted skimmers, a current reality and major concern for law enforcement.

Mutual device/host authentication

UDynamo is based on the MagneSafe Security Architecture (MSA). When configured for Security Level 3, mutual authentication is enabled. The host and uDynamo can engage in a cryptographic challenge and response sequence. Both the host and uDynamo can determine if the other is genuine. In security level 4, uDynamo is set to require authentication. In this mode, uDynamo will not turn on or transmit any swipe data until the authentication handshake with a valid host is complete.

UDynamo can manage session security, so that swipes can be time bounded. UDynamo can accept an encrypted session ID which is decrypted inside its security processor (inside the head) and returned to the host in the encrypted packet. At the host, the session ID status can be verified. If the session has expired, the swipe data can be ignored and the application can prompt for a fresh swipe. Time bound swipes effectively thwart malicious coders who try to trap an encrypted swipe and save it for future use.

uDynamo
SCRA with audio jack connection for iOS and Android devices

Anti-skimming features

MagnePrint, a counterfeit detection technology, transforms the encoded cardholder data – data that is static by nature – and makes it dynamic, much like a one-time password. Dynamic Digital Identification (DI) delivers unique data, each time a card is swiped based on the cards' MagnePrint. No two are ever repeated, and they can never be fabricated due to the natural, unique characteristics of the stripe, providing the best in counter skimming solutions. The MagnePrint or DI is a constantly changing value that transforms the magnetic stripe card into a unique, non-reproducible, dynamic token.

Counterfeit detection - cards and devices

uDynamo have the ability to see more data. They can read the encoded track data while simultaneously reading the underlying magnetic fingerprint. Every magnetic stripe card has a unique magnetic fingerprint which can be correlated to a reference print. With the ability to look at the magnetic fingerprint from each swipe and authenticate it against the original print, counterfeit cards can be detected at the point of use. The host can then alert the Merchant of the problem, letting it decide whether to accept the risk of a chargeback.

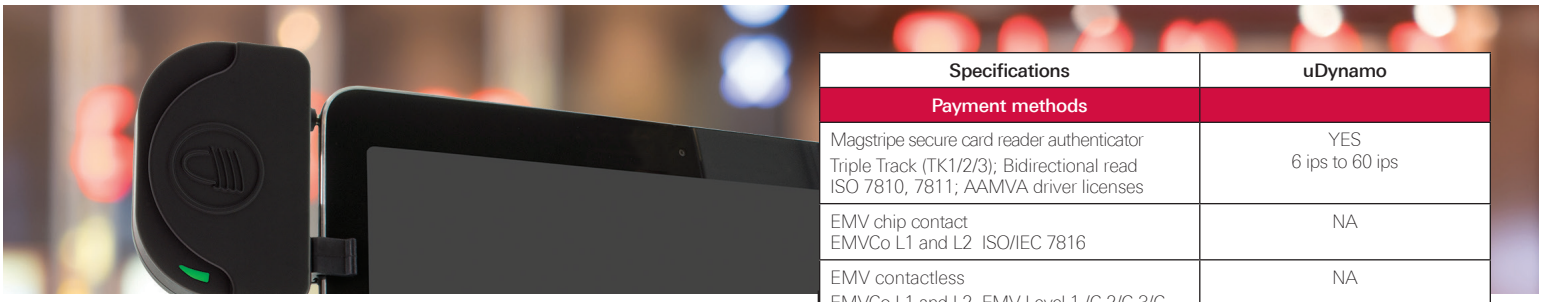
uDynamo determines if the data on the card has been altered. Tampered cards pose another problem at point of sale. While CVV1 and CVV2 can protect the account number, expiration date, and service code from alteration, uDynamo determines if any of the cardholder data has been altered.

Tamper resistant and tamper evident enclosure

UDynamo has been designed to deter physical intrusion by showing visible evidence if the outer cover has been opened. Since all of the data encryption occurs within the encapsulated read head, physical tampering would be obvious and likely harm the electronics which would render the reader inoperable.

Token generation

(the card, the PAN and the transaction)
Generating Tokens inside uDynamo at the point of swipe eliminates the need to contact a host for token generation.



Specifications	uDynamo
Payment methods	
Magstripe secure card reader authenticator Triple Track (TK1/2/3); Bidirectional read ISO 7810, 7811; AAMVA driver licenses	YES 6 ips to 60 ips
EMV chip contact EMVCo L1 and L2 ISO/IEC 7816	NA
EMV contactless EMVCo L1 and L2, EMV Level 1 /C-2/C-3/C-4/C-5 ISO/IEC 18092, ISO/IEC 14443 (Type A/B)	NA
NFC contactless / mobile wallets ISO/IEC 18092, ISO/IEC 14443 | (Type A, Type B) C-1/ C-6/C-7 D-PAS®, PayPass™, payWave®, ExpressPay®, Apple Pay ®	NA
Reliability and Operation	
MSR / SCRA swipes	1 Million
EMV insertions	NA
Operating System	Windows plug & play
CPU and memory	Non-volatile
Status indicators	Status LED (Red/Green/Amber)
Device Compatibility	Windows, Android, iOS
General	
Connection Method	Retractable Audio jack USB micro B
Wireless (Frequency 2.4 MHz)	NA
Interface	USB Micro B, Audio jack
Display	NA
Secure Key Pad	NA
Optional Accessories	NA
Web services	Magensa Services
Electrical	
Charging	Rechargeable Micro-USB charge
Battery	Li-ion Polymer
Current and Power	Power via USB or Battery. 100 mA max
Security and Certifications	
Compliance (FCC, CE, UL)	YES
Data protection 3DES encryption; DUKPT key management MagneSafe Security Architecture Unique, non-changeable device serial number	YES
Tamper	Evident/Resistant
Mechanical	
Dimensions L x W x H or L x W x D	2.5 x 1.55 x 0.62 in 63.5 x 39.4 x 15.7 mm
Weight	1.036 oz. (30 g)
Mount/Stabilizer	Stabilizer clip
Environmental	
Operating temp	32°F to 113°F (0°C to 45°C)
Operating humidity non-condensing	10% to 90%
Storage temp	14°F to 140°F (-10°C to 60°C)
Storage humidity non-condensing	10% to 90%

MAGTEK®
SECURITY FROM THE INSIDE

Founded in 1972, MagTek is a leading manufacturer of electronic systems for the reliable issuance, reading, transmission and security of cards, 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, token generators, EMV contact, contactless 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, and processors to provide secure and efficient 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 online identification, payment processing, and high-value electronic transactions.