MAGTEK®
SECURITY FROM THE INSIDE

Product List

- Magnesafe IntelliHead Components
  - USB
  - SPI
  - UART

OEM MagneSafe Components

IntelliHead USB, SPI, UART Components
Magnetic Stripe Reading

MagneSafe® IntelliHead is the industry's first magnetic sensing, media validating, tamper resistant security module. It is more than just a magnetic read head. It delivers unmatched protection from the inside by capturing more robust magnetic information for next generation security solutions. This heavy-duty small bracket holds a pre-aligned reader/authenticator ready for snap-in installation. All of its processing power and communication circuitry is located within the mounted authentication sensor. As a result, the MagneSafe IntelliHead sets new standards for small size, security, increased noise immunity and excellent environmental resistance all with complete compatibility to existing reading applications.

MagneSafe Security Architecture is a foundation you can build on. The MagneSafe Security Architecture has evolved exponentially from its inception in 2006 when it delivered the industry's first Secure Card Reader Authenticators (SCRAs) for secure electronic transactions.

CALL - 562.546.6400 | EMAIL - oem.solutions@magtek.com

MagneSafe is a digital identification and authentication architecture that safeguards consumers and their personal data. Designed to exceed PCI regulations, MagneSafe Security Architecture (MSA) leverages strong encryption, secure tokenization, counterfeit detection, tamper recognition, data relevance and integrity, and dynamic digital transaction signatures, which together validate and protect the entire transaction and each of its components.

Secure and Reliable

The multi-layer security MagneSafe adds unmatched protection both cardholders and relying parties require through sophisticated card, device and data authentication methods that assure a valid transaction. MagneSafeis based on technology that makes cardholder data harder to acquire and dynamic, rather than static, eliminating its redemption value if stolen. MSA uses encryption for a preventive measure that protects cardholder data at rest and in transit at various points through the payment infrastructure and authentication that protects cardholder data that exists outside of the network.

The technology, MagnePrint®, is a card authentication, patented, and proven technology which reliably identifies counterfeit credit cards, debit cards, gift cards, ATM cards and ID cards at the point of swipe, before fraud occurs.

Strong Encryption

MagneSafe encryption scrambles the data at the point of swipe, providing instant protection. Without the secret key, the data is unreadable and never in the clear. By using strong industry standard encryption algorithms along with sound key management, MagneSafe protects cardholder data from prying eyes and eavesdroppers.

Counterfeit Detection

MagneSafe verifies legitimate cardholder data by successfully identifying the card's unique features and proving its authenticity.

Tamper Recognition

MagneSafe recognizes tampered cardholder data and assures that transactions are only performed using legitimate, unaltered cardholder information.

Data Relevance and Integrity

MagneSafe validates the relevance and integrity of the cardholder data gathered by a swipe, dip or insertion of a card. To know that the data is fresh, the reader itself supports mutual authentication, session management, and data integrity verification.

Secure Tokenization

MagneSafe supports secure tokenization so merchants and retailers do not have to store the actual PAN data on their host system. A unique "token" is generated with each swipe and it is this token that is used for settlement purposes or to retrieve information for charge backs so the data is never out "in the clear."

Dynamic Digital Identification

MagneSafe offers data obsolescence or auto-expiration by generation of dynamic authentication transaction values that change with each swipe of a card. This method assures that the cardholder track data is genuine – and has not been obtained from a breach or from a counterfeit card.

Device Authentication/Host Authentication

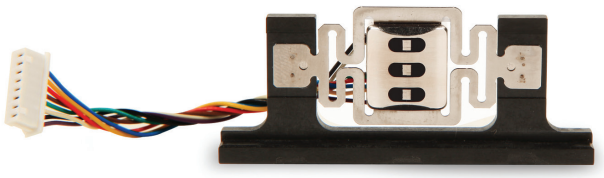
MagneSafe readers can be configured to authenticate a host before sending the encrypted card data. This type of authentication requires a mutual handshake between the MagneSafe reader and the host, eliminating the threat of being re-directed to an illegitimate host. Furthermore, the device itself can be authenticated so the host may know it is a valid reader-authenticator.

Ready for Integration

MagneSafe IntelliHead is security built into MagTek's line of Secure Card Reader Authenticators (SCRAs). MagneSafe SCRAs deliver dynamic card authentication, data encryption, tokenization, and device/host authentication to protect cardholders from identity theft and card fraud. MagneSafe SCRAs deliver a variety of configuration choices with unmatched reliability and first swipe read rates. Integrate MagTek components and devices into your solution easily with APIs, software developer kits and MagTek support services.

No other Technology Does More

When it comes to protecting cardholder data at the point of transaction, no other technology does more than the MagneSafe Security Architecture. The MagneSafe IntelliHead is built into MagTek secure card reader authenticators, PIN devices (including DynaPro and DynaPro mini) and insertion readers (including Perma Seal and Slim Seal) and is ready for integration.



MagneSafe IntelliHead Accordion Spring U-bracket

SPI connection (UART, USB not pictured)

MagneSafe IntelliHead Butterfly Spring

USB, SPI, UART connections available

MagneSafe IntelliHead Accordion Spring U-bracket

USB Connection (UART, SPI not pictured)

Features

- Ideal for PCI applications
- Open standards-based encryption 3DES (TDEA)
- DUKPT Key Management
- MagnePrint® Card Authentication
- Tamper Resistant Security Module (TRSM)
- Immediate card data tokenization
- Protects card data per PCI DSS requirements
- Generates dynamic data with each swipe
- Device/host authentication
- Unique, non-changeable serial number
- Time bound session IDs
- Quick testing and start up
- Remote key loading (USB devices only)

Specifications

Read: Bi-directional card reading

Ref Standards: ISO 7810 and ISO 7811/ AAMVA*

Tracks: Reads up to 3 tracks of data

Message Format: ASCII

Reliability: 1 Million swipes

* ISO (International Standards Organization)
* AAMVA (American Association of Motor Vehicle Administrators).

SECURITY

Key Management: DUKPT

Encryption: 3DES encryption

ENVIRONMENTAL

Humidity Operating & Storage: 10% to 90% noncondensing

REFERENCE STANDARDS AND CERTIFICATIONS

- FCC Title 47 Part 15
- CE class B
- CE Safety
- UR/CSA
- (RoHS) European Directive 2002/95/EC

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. MagTek is headquartered in Seal Beach, CA.