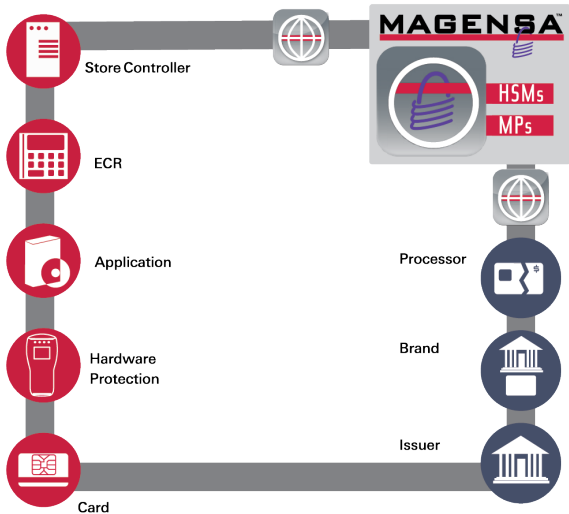# MAGTEK®
SECURITY FROM THE INSIDE

Magensa Retail POS
Secure Rail for the Point of Sale

Encryption and secure tokenization of cardholder data has become an important component in the retail environment to provide protection and meet compliance measures such as those issued by the PCI SCC. When strong encryption and secure tokenization are used in conjunction with dynamic card authentication, it provides a solution that can protect cardholder data while at rest or in transit. It further secures payment systems with real-time information to prevent, detect and alert to the presence of fraudulent transactions and rogue devices.

The MagneSafe™ Security Architecture (MSA) is the foundation that Magensa Service is built on. The MSA has evolved exponentially from its inception in 2006 when it delivered the industry's first Secure Card Reader Authenticators (SCRAs) for secure electronic transactions. The MSA is a digital identification and authentication architecture that safeguards consumers and their personal data. Designed to exceed PCI regulations, 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.

A key feature of the MSA is MagnePrint® card authentication, a patented, 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. MSA's multi-layer security provides unmatched protection and flexibility for safer online transactions. The MSA comprehensive approach to transaction security makes stolen cardholder data useless to criminals and ultimately reduces the incentive to steal it.

MAGENSA™

HSMs
MPs

Store Controller

ECR

Application

Hardware Protection

Card

Processor

Brand

Issuer

Magensa Secure Rail
Flexible and scalable to meet your needs

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

Magensa provides risk mitigation and fraud prevention along the POS rail, providing greater transaction control and easier integration based on your unique needs. Magensa's real-time forensics prevent fraud, making it substantially easier for law enforcement to track and find fraudsters.

Magensa is scalable and flexible. Merchants can use combinations of services at differing levels including: Hardware and Services (decrypt, tokenize, authenticate, remote services); Gateway Services (MPPG, Decrypt and Forward); and Application layers.

Brick and mortar POS
- Exceeds current PCI requirements
- Combats thievery of unencrypted data
- Uses triple DES encryption
- Provides an open solution

Encrypted contactless
- Exceeds PCI DSS requirements for securing cardholder data
- Guards against RFID skimming
- Makes stolen card data useless to thieves

Gas pumps and unattended kiosks
- Deters card skimming, rogue devices and fraudulent cards
- Provides card authentication
- Stops fraudulent transactions in real-time

Card present Internet payment
- Delivers secure online transactions
- Authenticates device/host
- Guards against phishing and other forms of cyber attacks
- Secures data with strong encryption

Legacy POS terminal
- Provides a fast track to PCI compliance
- Simplifies the upgrade process
- Extends the value of current terminals

Mobile POS
- Provides a pocket sized reader for on-the-go mobile merchants desiring PCI DSS secure card present transactions
- Securely upload the encrypted transactions at a later time for payment processing

Private label and gift card issuance
- Delivers personalized cards that earn "top of wallet"
- Captures dynamic digital identifiers for card authentication
- Secures operations with remote activate/deactivate feature

Remote key injection
- Provides secure remote key management
- Authenticates devices

- Minimizes risks
- Enhances operations
- Saves time and resources

Remote device configuration
- Eases deployment and device management
- Authenticates devices
- Minimizes risks
- Enhances operations

Virtual terminal (PC POS)
- Transforms any browser into a secure POS application
- Adds dynamic data to each transaction
- Makes cardholder data useless to criminals

Wireless POS
- Communicates with a PC or mobile phone using a secured wireless USB interface or Bluetooth interface
- Provides secure, card present data for pay-at-the-table and mobile users