MAGTEK®
SECURITY FROM THE INSIDE

MagTek's Magensa Services

Transaction Security Services

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.

Magensa is a subsidiary of MagTek, Inc.

Magensa™ is a fraud prevention, detection and advisory service. It maintains a globally accessible registry of authentication information so that consumers, financial institutions, retailers, businesses and governments can assess the validity and trustworthiness of the credentials and products they rely upon in the course of online identification, payment, and other important transactions.

Magensa provides token management and cryptographic services, vital to the protection of cardholder data, the payment system, and personal or sensitive information.

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

Partnership

Magensa is your partner, not just a service provider.

Magensa is a service that maintains PCI compliance at all times. We do more than just protect cardholder track data at our geographically separated and redundant data processing facilities. You don't need to wait for anyone else in the transaction process to take advantage of the benefits that Magensa and the MagneSafe™ Security Architecture (MSA). MSA delivers security and a return on investment where it matters most to you with guaranteed returns.

Tested and Proven

Magensa delivers industry standard and best practice solutions. Magensa's data protection, tokenization, encryption, authentication with registration, and enterprise device management services secure today's traditional applications with tomorrow's advanced security requirements. These secure services protect sensitive data at every point of the transaction, increase brand value, counter skimming solutions and limit fraud and theft with minimal improvements to the payment infrastructure.

Return on Investment

Magensa gives you the ability to fight fraud and earn rewards. Magensa provides Code 10 fraud alerts for counterfeit cards with the forensic evidence to stand up in court.

Magensa and You

Magensa's Technical Support Team works with you to assess your current environment and develop implementation and deployment strategies for your unique organization. Your representative will work with you to the path of success.

Best in Design and Operational Practices

We take transaction security seriously and understand that your security system extends beyond the purchase and extends into a lasting relationship. You require business continuity, agility and a team working for you.

Around-the-Clock Customer Support

We work around the clock to ensure constant, consistent and reliable service. We understand that time is money and strive to provide a synergistic solution that brings your services to the next level. After a customer, you will be provided with a dedicated support number you can contact 24/7/365 for software support and online diagnostic capabilities.

Excellence in Functionality

Save time and resources while receiving around the clock, reliable 99.99% uptime and guaranteed service. Our Secure Data Center operates 24 hours, 7 days a week, 365 days a year with full staff management and technical support. We offer a layered defense with automatic fail-over, load balancing, device and location independence, automatic back-ups and redundant data processing facilities.

Complete Scalability and Integration

Magensa offers scalability of services and of resources. Depending on your individual custom needs we will work with you to provide a custom turnkey solution so you don't have to build extraneous support. We deliver scalability via dynamic provisioning of resources, secure multi-tenancy and around the clock performance monitoring.

Magensa Payment Protection Gateway

Magensa's Payment Protection Gateway (MPPG)

MPPG makes PCI compliance easier, safer and faster with a flexible and safe way to conduct payment transactions. The Magensa Payment Protection Gateway can work as your secure rail to send data onto processors, gateways and acquirers. Data is sent through an open and secure platform from all MSA enabled terminals making it the most secure gateway in the industry today.

The Global MagnePrint Exchange Service

Magensa's Global MagnePrint Exchange Service is a shared, accessible fraud information database. It stores and accesses data pertaining to devices and cards that use the MSA. The Global MagnePrint Exchange Service prevents fraud that would occur from skimmed cards using a combination of dynamic card data, authentication, tokenization and encryption services. This service protects you whether you are paying for gas at an unattended gas pump or in a store handing your card to a cashier.

PCI Compliant and Reduced PA DSS Scope

Magensa simplifies PCI compliance, reduces your PCI scope* and decreases costs by as much as 50-75%. The use of MagTek's MagneSafe Security Architecture (MSA), in combination with our certified Magensa Payment Protection Gateway (MPPG), may allow customers employing these systems together, to reduce or entirely remove their application from the scope of PA-DSS compliance. By encrypting the card data at the earliest possible point (inside the read head and at the moment of swipe), using an industry standard encryption method (3DES), dynamic encryption keys (DUKPT), and not providing the encryption key to the application vendor, MagTek and Magensa are following the best practices accepted in the industry regarding Point to Point Encryption.

MagTek and Magensa go beyond this level of encryption security however, by providing token services, and card authentication services (MagnePrint®) based on dynamic payment card data.

"We believe the PCI Security Standards provide a solid foundation for a security strategy to look after your payment and other types of data, but security does not start and end with compliance. Focus on good security and compliance will follow."

- Bob Russo, General Manager of PCI DSS,

MagneSafe™ Security Architecture

The MagneSafe Security Architecture is the foundation that Magensa is built on. The MagneSafe Security Architecture (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.

It has always been part of MagTek's mission to lead the way in terms of card data security and by providing additional card security features; now the MagneSafe Security Architecture can help future proof your application in an ever-changing environment.

Software developers that do not want to go through PA-DSS should exclude the collection of Payment data in their applications. Instead, they should use Secure Card Reader Authenticators (SCRAs) and a virtual terminal like that provided by Magensa to collect and process cardholder data. If their application collects cardholder data, even if encrypted, according to PCI they must comply with PA-DSS.

* See complete statement in doc PN 99800063.

Industry experts agree that a layered approach is the best approach for security and MagneSafe provides the layers necessary in one easy to implement, scalable solution. SCRAs provide true end-to-end encryption with the encryption occurring within the reader, along with tokenization formatting capabilities.

Encryption and tokenization are preventive measures that help to protect cardholder data, at rest and in transit, and at various points through the payment infrastructure. Encryption and Tokenization, do not protect cardholder data that exists outside of the network. Here data is widely available from other data capture venues such as pocket skimmers, unattended gas pumps, phishing and pharming sites, and telephone scams.

The multi-layer security of MagneSafe adds the unmatched protection both cardholders and relying parties require through sophisticated card, device and data authentication methods that assure a valid transaction.

The MagneSafe Security Architecture works with the 5.5 billion magnetic stripe cards already in circulation including those coupled with EMV and contactless NFC EMV.

SCRAs deliver dynamic payment card data (digital identifiers of ID), and magnetic card stripe fingerprinting (MagnePrint) which provides counterfeit detection, counters skimming attempts and stops fraudulent transactions in real-time. No other security device in the market today is able to do everything that MagneSafe™ does in one easy to implement, scalable, cost-effective solution.

MagneSafe SCRAs transform the existing magnetic stripe card into a highly secured payment and identification token with proven ability to identify counterfeit cards and prevent card fraud.

Data Protection

Secure your sensitive data, increase customer confidence, exceed current PCI DSS requirements and expand your market while maintaining a return on your investment using Magensa's Data Protection services. Magensa's Data Protection services combine a layered approach to secure sensitive data. Data is protected at all times, whether at rest or in motion from the earliest point of the transaction. The use of encryption and tokenization when combined with dynamic authentication, protects cardholder data throughout the payment infrastructure.

Encryption and Decryption

Magensa's encryption and decryption services deliver practical solutions for data protection that exceed current PCI DSS regulations. Magensa utilizes open standard and industry proven Triple DES encryption and DUKPT (derived unique key per transaction) key management to provide a comprehensive security solution that protects cardholder data while at rest and in motion from the earliest point of the transaction. Its open platform does not require you to invest in costly, untested, proprietary solutions that can limit your long-term flexibility and options. Magensa can have you up and running in a matter of hours.

Using devices secured by the MagneSafe™ Security Architecture, encryption occurs directly in the read head at the point of swipe, protecting the data instantly and exceeding PCI requirements because data is never in the clear. After the encrypted data is securely delivered to Magensa, transactions can be securely decrypted and then delivered to the appropriate payment gateway or processor.

Tokenization and Masking

Magensa's secure tokenization and masking services provide you with the next level of a layered defense. In today's world, storing clear text cardholder data opens the door to fraud, brand damage and the potential for massive fines. Magensa provides secure Tokenization so merchants and retailers do not have to store the actual PAN data on their host. During the transaction, the cardholder data is encrypted and is assigned a unique "Token" generated by a one way encryption algorithm. The token could be used for settlement purposes or to retrieve info for charge-backs without having to obtain or store PAN info "in the clear."

Secure Data Storage

Magensa does not store clear text cardholder data. All data is encrypted using industry proven Triple DES encryption and DUKPT (derived unique key per transaction) key management and it uses a unique token to identify all cardholder sensitive data.

Magensa provides authentication for personal electronic devices including, smartphones, PCs, payment terminals, PIN encrypting devices, card and check readers, servers, and card issuing units. Legitimate devices, including mobile on-the-go POS devices (including Android smartphones, and many iOS devices) using a connected secure card reader authenticator, can be identified and authorized for use while rogue devices can be identified and stopped before they are used to commit fraud.

Device Management

Know that the devices you are communicating with are legitimate. Device management goes beyond merchant IDs and terminal IDs and makes it impossible for rogue and tampered devices to communicate with your network. Using a proven mutual authentication technique, secured devices are programmed to generate an encrypted challenge and communicate directly to Magensa. This mutual authentication allows both the user and the host to validate their identities. If one does not recognize the other as legitimate, the authentication will fail and the device will be disabled.

Remote Services

Save time and resources with secure remote key injection and key management. MagTek's secure infrastructure allows institutions to safely and remotely inject encryption keys and manage devices, minimizing risk, lowering costs and enhancing overall operations. Using a proven, robust mutual authentication technique, secured devices allow both the user and the host to validate their identities. If one does not recognize the other as legitimate, the authentication will fail and the device will be disabled.

Remotely enable a device for operation. Magensa can be programmed to remotely enable and configure your device for operation. After the device and Magensa have been mutually authenticated, a digital certificate is transmitted to the device, enabling it to operate for a user defined period of time. Magensa can use the same infrastructure to configure and disable a device and it will remain non-operational until it is re-enabled. This service mitigates your liability and allows you to remotely control any device connected to the network.

Digital Signatures and Session IDs

Protect your data from redirection and guard against in-transit data attacks and prevent man-in-the-middle attacks using session IDs and digital signatures.

Key Injection and Life Cycle Management

Magensa delivers protection against third party and rogue devices by providing secure initial key injection and life-cycle management.

Digital Device Solutions

Magensa supports an array of electronic devices including POS terminals, PCs, ECRs, card readers, PIN encrypting devices, credential personalization and issuing devices, secure card reader authenticators, small document scanners, and most any electronic transaction device connected to the internet (including smartphones and PCs).

Authentication & Registration

Magensa's Authentication and Registration services prevent fraud using MagnePrint® as a risk management tool. This layer of protection, when properly implemented, will detect skimmed or magnetically altered counterfeit cards in real-time and stop transactions before fraud occurs. Our real-time fraud alerts protect you from chargebacks, tampering, illegal (rogue) devices, unauthorized devices, replays, expired sessions, counterfeit cards, illegal and out of pattern usage preventing fraud, and providing a true return on investment. Magensa also provides the best in custom analytical reporting so you get the information you need, when you need it, saving time and resources.

Global MagnePrint® Exchange Service

Magensa operates the world's largest open and shared registry of magnetic fingerprints for ATM, credit, debit, gift and loyalty cards, allowing financial institutions and merchants around the world to immediately distinguish between an original and a counterfeit card. When payment cards are used, a magnetic fingerprint (MagnePrint) is captured and sent to Magensa for comparison and scoring. Each MagnePrint is unique, even if card data has been stolen or skimmed, the counterfeit card will never match the original reference print.

MagnePrint Risk Management Services

Maintain security and prevent fraud while increasing consumer confidence with solutions that go beyond current PCI DSS compliance measures.

Card Credential Registration Services

Registration is the backbone to authentication and can be implemented easily without the need to re-issue cards. Card credentials can be registered with Magensa at the point of issuance or in the field. MagneSafe™ technology makes in the field registration possible by transmitting the authentication data at every point of swipe. The database becomes populated over the course of time during normal use, eliminating the need to re-issue cards. The database then provides the basis for authentication.

Card Credential Authentication Services

Card authentication allows any participant in the payment process to affirm the physical card is genuine and has not been cloned or altered. Magensa uses the MSA to safeguard consumers and their personal data.

Authentication Scoring Services

After card credentials are registered, transactions can be scored based on the authentication data created at the point of swipe and can be assessed and scored against the intrinsic characteristics that correlate to the registered card.

Dynamic Digital Identifiers

MagnePrint transforms cardholder data each time a card is swiped. No two MagnePrints can ever be repeated due to the stochastic properties of the magnetic material, the unique property of each individual swipe, and DUKPT key management.

Two-factor Authentication

Two-factor Authentication provides a more secure vehicle for data access protection and is recommended by the FFIEC. This layer of security is made possible by combining dynamic card authentication (something you have which cannot be duplicated) with a password (something you know).

Flexibility

eCOMMERCE: Magensa's unique ability to track transactions in real-time, per transaction and per device, make it an ideal companion to the buying and selling of goods and services online. It delivers the tools you need for the development, marketing, selling, and delivery of online goods and services, retail services, marketplace services, mobile commerce, and e-Procurement.

RETAIL: 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. Magensa allows you to implement risk mitigation and fraud prevention at the POS, store controller, merchant host, processor/gateway, acquirer, brand switch, or issuer, 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.

FINANCIAL: Create a finance environment that enhances brand reputation and depositors' experience. Leveraging the power of the MagneSafe™ Security Architecture, you can exceed current FFIEC recommendations for two-factor authentication and secure the in-branch and remote electronic banking environments with cost effective solutions that leverage cards already in circulation. Magensa allows you to implement risk mitigation and fraud prevention in ATMs, online, mobile, remote deposit capture and in-branch services including teller windows, card personalization and card issuance.

ENTERPRISE: Magensa delivers risk mitigation and fraud prevention for IT content and delivery management, facilities access control, forms management, intellectual property management, new hire ID verification, user identities and remote user and employee accesss. Magensa's real-time authentication makes it substantially easier for IT departments to manage their users and resources.

GOVERNMENT: Magensa provides mitigation and fraud prevention for Alcohol/Tobacco/Firearms, DMV, elections, legislative regulations, social security, TSA and remote employee/user access.

Magensa services provide greater transaction control and easier integration based on your unique needs.

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.

MagTek, Inc. | www.magtek.com |