MAGENSA™

A MAGTEK COMPANY

Payments

Integrated Transaction Security

Simplified PCI and EMV Readiness for Payments

MagTek services are backed by over 48 years of industry know-how with solutions to meet your needs for payment processing. MagTek's hardware and Magensa's Services create a scalable and flexible payment ecosystem. MagTek delivers secure point-of-sale and point-of-service (POS) devices and Magensa delivers decryption, gateway, and application services. All of these solutions protect card data at the earliest point possible, lower scope of PCI compliance, deliver P2PE validated key injection services, and provide a path forward to support the adoption of a magstripe, EMV Contact Chip, EMV Contactless, NFC, and Secure Manual Entry payment infrastructure. Together we work with affiliates who are leaders in the industry to deliver excellence in design, exceptional support, and secure, reliable products.

Security from the inside.

MagTek's key differentiator is "Security from the Inside." Since our founding in 1972, MagTek has been a leading secure payment solution provider in the industry. The exclusive feature that continues to set MagTek apart is our MagneSafe® Security Architecture. These secure services protect sensitive card, chip and token data at every point of the transaction, increase brand value, counter skimming, and limit fraud.

MagneSafe Security Architecture

MagneSafe is a digital identification and authentication architecture that safeguards consumers and their personal data. Designed to exceed PCI regulations, MagneSafe 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. MagneSafe Security Architecture allows our partners to exceed PCI DSS standards. Every merchant realizes a positive ROI quickly with MagTek's POS solutions by ensuring a merchant's POS system is free and clear of cardholder data. MagneSafe's multi-layer security provides unmatched protection and flexibility for safer digital transactions. Combining the power of MagneSafe with the Payment Protection Services of Magensa, users gain the benefit of a trusted and proven solution that is affordable, scalable, and easy to deploy.

Simplifying payments world wide

Magensa offers a partner agnostic approach with open standards encryption and back end data routing. Serving enterprises globally, Magensa provides a wide range of innovative tools and transaction processing services for authentication, cryptographic security, and privatization of sensitive data. Magensa's encryption/decryption services, payment gateway services, tokenization services, remote services, and applications are used by software developers, ISVs and systems integrators to bring their applications to market faster and more securely. These secure services protect sensitive data at every point of the transaction, increase brand value, counter skimming and limit fraud and theft with minimal improvements to the payment infrastructure.

Cardholder Data Environment (CDE)

Magensa's Services deliver a no CDE. The CDE is an, "...area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment."

This enables Magensa's users to deploy multiple, low-cost, yet secure point-of-service payment devices directly to the customer wherever and whenever they are ready to buy: increasing convenience; speeding check-outs; enhancing security; reducing the overall risk of fraud; all while limiting the scope of PCI.

Data Security Services

Secure your sensitive data, increase customer confidence, and expand your market while maintaining a return on your investment using our data protection services. Data is protected at all times, whether at rest or in motion from the first point of the interaction, simplifying P2PE development. The use of encryption and tokenization, when combined with dynamic authentication, protects cardholder data throughout the payment infrastructure.

Magensa Device Authentication: Magensa delivers protection against rogue devices by providing secure key injection and mutual authentication between the payment device and the Magensa Host.

Magensa Decrypt Service: Magensa's Decryption Services deliver practical solutions for data protection that exceed current PCI DSS requirements. Magensa utilizes open standards Triple DES encryption and DUKPT (derived unique key per transaction) key management to provide a comprehensive security solution that protects cardholder data with dynamic encryption from the earliest point of the transaction.

Gateway Services

Magensa's Gateway Services are cost-effective, easy to use, and reduce integration time.

Magensa Decrypt and Forward Gateway

- Decrypt and Forward allows merchants to securely integrate encrypted card swipe data into a payment application where the payment application traditionally transmits unencrypted card swipe data when calling web services for a third-party service provider. This process will allow a user to support encrypted card swipe data in their payment application without the third-party service provider supporting a decryption service.

Magensa Payment Protection Gateway (MPPG)

- MPPG is an extensive set of web services used by Point of Sale (POS) systems to secure and authorize credit card payments for mobile, e-commerce, or traditional brick and mortar stores. Magensa's Payment Protection Gateway (MPPG) makes EMV adoption and PCI compliance easier, safer, and faster with a flexible and safe way to conduct payment transactions using a variety of payment instruments. Magensa Payment Protection Gateway works as your secure rail to send data onto other acquirers, gateways and processors. Data is sent through an open and secure platform from all MSA enabled payment devices making it the most secure gateway in the industry today.

	Service - Level 1 Service Integration Hardware/Service	Service - Level 2 Semi Integration Hardware/Service/ Gateway	Service - Level 3 Full Integration Hardware/Service/ Gateway/Application
PCI Scope	Cardholder data never enters the Merchant environment	Cardholder data never enters the Merchant environment. Cardholder data is secured through the gateway.	Cardholder data is secure through the entire payment ecosystem. The point of sale software infrastructure is reduced from PA-DSS scope.
Hardware PED hardware is reviewed by PCI-DSS	APIs / SDKs Drivers for MagneSafe POS hardware	APIs / SDKs Drivers for MagneSafe POS hardware	APIs / SDKs Drivers for MagneSafe POS hardware
Security **Tokenization** **Authentication** **Administrative** **Services** **Decrypt**	APIs / SDKs Scoring Risk assessment Fraud Alerts Remote Key Injection Device Configuration	APIs / SDKs Scoring Risk assessment Fraud Alerts Remote Key Injection Device Configuration	APIs / SDKs Scoring Risk assessment Fraud Alerts Remote Key Injection Device Configuration
Gateway **Decrypt & Forward** **MPPG**		Decrypt and Forward or Magensa Payment Protection Gateway	Decrypt and Forward or Magensa Payment Protection Gateway
Software App **Identity & Access Mgmt** **Payment App** **eSignature** **Issuance**			Point-of-sale/Point-of-service application QwickPAY, QwickSIGN & Pay, QwickCards

Service Level 1 - Service Integration
Hardware | Services

1. Card Reader/POS app
Sends encrypted data

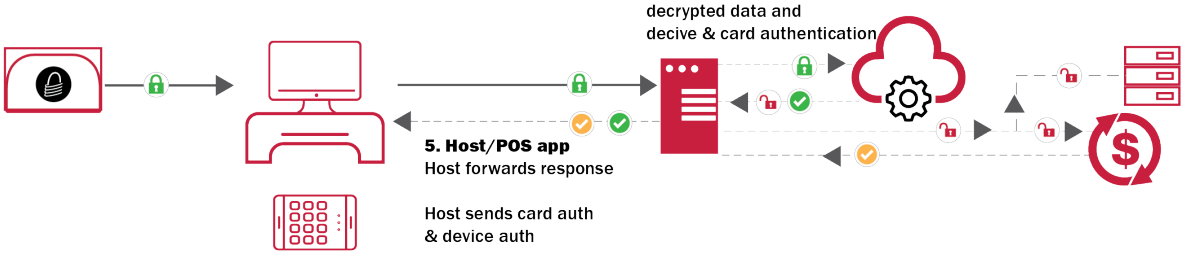
2. POS app/Host
Sends encrypted data

3. Host /Magensa
Host sends encrypted data to Magensa

Magensa returns decrypted data and decive & card authentication

4. Host/Processor/other
Host sends to other/processing

Other/processor send response back to host



5. Host/POS app
Host forwards response

Host sends card auth & device auth

Card Reader
eDynamo

POS application
Countertop or
Mobile Device

Central Host
Networked

Magensa Web Service
Decrypt

Processor/Other

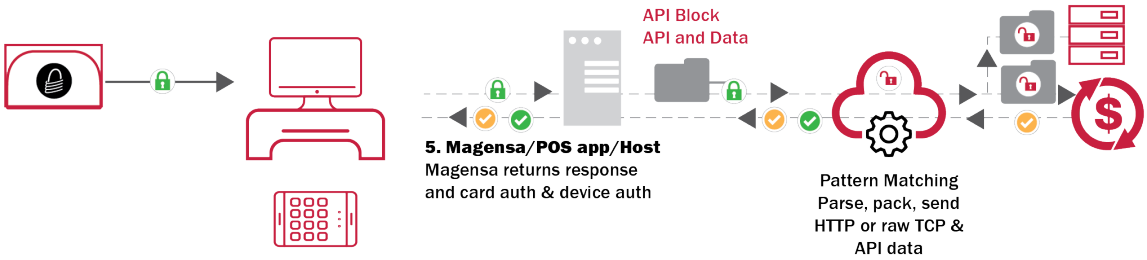
Service Level 2 - Semi Integration
Hardware | Services | Gateway

1. Card Reader/POS app
Sends encrypted data

2. POS app/Magensa
POS app/Host send encrypted data and API block to Magensa

3. Magensa
Magensa decrypts, bundles with APIs and sends out for processing or other transaction types.

4. Processor/other
Processor/other sends response back to Magensa



5. Magensa/POS app/Host
Magensa returns response and card auth & device auth

Pattern Matching
Parse, pack, send
HTTP or raw TCP &
API data

Card Reader
eDynamo

POS application
Countertop or
Mobile Device

Optional Host
POS app and/or
central host

Magensa Web Service
Decrypt and Forward

Processor/Other

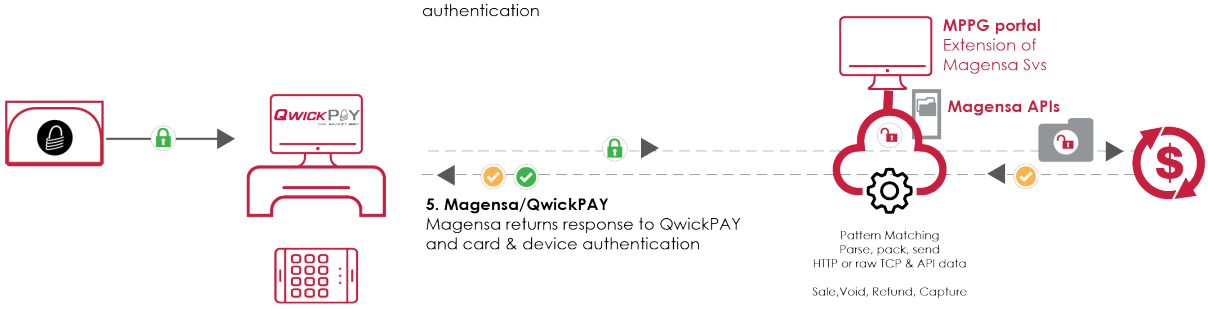
Service Level 3 - Full Integration
Hardware | Services | Gateway | Application

1. Card Reader/POS app
Sends encrypted data

2. QwickPAY/Magensa
QwickPAY/POS app sends encrypted data to Magensa to perform transactions and card & device authentication

3. Portal /Magensa
Magensa decrypts, bundles with Magensa APIs and sends out for processing.

4. Processor
Processor sends response back to Magensa



5. Magensa/QwickPAY
Magensa returns response to QwickPAY and card & device authentication

Pattern Matching
Parse, pack, send
HTTP or raw TCP & API data

Sale,Void, Refund, Capture

Card Reader
eDynamo

POS application
Countertop or
Mobile Device

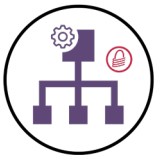
Magensa Web Service
Magensa Payment
Protection Gateway

Processor

Magensa Tokenization

Magensa provides secure Tokenization Services so merchants do not have to store the actual PAN data on their host. Tokenization enables users to limit or entirely remove sensitive card data from their domain by substituting non-sensitive data that is used in place of clear-text card data. The tokens are used for a variety of transactions including recurring payments, chargeback disputes, loyalty and reward programs, and other uses where merchants want to minimize their overall risk for being the source of a data breach. Magensa's tokens are vaultless. The token itself securely encapsulates the cardholder data, encrypted by a unique key used only once. Because of dynamic key management, it would be a nearly impossible and highly expensive task to break any token. The primary benefit of tokenization is to reduce the scope and footprint of PCI-DSS audits and therefore its associated costs.

By limiting or removing sensitive card data from their domain users save significant time when conducting annual compliance audits. With proper planning, many users have gained significant reduction in scope of their PCI-DSS compliance audits and in some cases, saved more than 50 percent. The key to reducing the PCI-DSS footprint is to never have access to the clear-text card data. If users encrypt card data when the card is swiped and receive a token in exchange, the user greatly reduces their PCI-DSS scope provided they demonstrate they do not have access to decryption keys or token vault.



Remote Services

Magensa's Remote Services are a convenient and secure solution for remote device configuration options and key inject encryption into SCRAs and PIN pad devices anytime, anywhere without the need to return the devices to the factory, lowering handling and shipping costs while increasing security and overall convenience.

Software and Applications

MagTek understands that without an application the best hardware in the world won't work. MagTek engineers products so they are easier to communicate with, better at understanding commands, and work with apps for fast deployment. Offering a line of applications for payments and issuance to better service you, whether you are a developer or an end user.

Developer Tools and Hardware

Developer Apps and Tools

MagTek is your partner in development and provides a comprehensive platform of drivers, APIs, and Software Development Kits (SDKs). The SDKs include tools, documentation, and sample code for developing applications in a variety of environments for fast development and easy integration. MagTek offers support from testing and integration, during roll out, and with training collateral, support guides, defined process for ordering new/replacement terminals, warranty details and life-cycle management processes. Magensa's MagneFlex and Wedget developer tools make integration easier.

Hardware Product Lines

Magensa offers a wide variety of development tools to easily integrate a wide array of MagTek devices across multiple platforms and operating systems. MagTek products include:

- OEM components,
- Encrypting check scanners,
- Secure magstripe, EMV chip, NFC readers, this Secure Card Reader Authenticator family of products give users the flexibility needed to securely accept a variety of payment card technologies.
- PIN encrypting devices. PIN Encrypting Devices (PEDs) are ideal for credit, ATM, Prepaid, gift, and debit cards for traditional or mobile point of sale applications where users need unmatched convenience & security.

Secure Manufacturing.

MagTek's state-of-the-art manufacturing and headquarters are located in Seal Beach, CA where engineering, design, final assembly and key injection occur.

- ISO 9001:2015 and TR39 certified facility.
- Chain of custody is second to none with secure carrier and distribution partners, tamper proof and/or tamper evident packaging.
- Devices are configured to require secure activation with mutual authentication.
- MagTek's Factory Key Injection and Magensa's Remote Key Injection services are both in compliance with TR-39/ PCI PIN requirements, and are re-validated for compliance via external audits.
- Magensa is a PCI Level 1 service provider and VISA TPA Program (ESO) Service Provider.

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.

  PN D998200060 rev 40 10/21