MAGTEK®
SECURITY FROM THE INSIDE

Software

MagneFlex Middleware Payment Application

MagneSafe Secure Eco-System

Hardware, Services, Gateway, and Application for a Complete Payment Solution

MagTek provides hardware characterized by "security from the inside" meaning its hardware protects cardholder and sensitive data at the absolute earliest point of contact. Our MagneSafe® enabled devices secure the data within the magnetic head. The secret keys used to prime the NIST (National Institute of Standards & Technology) approved algorithms are loaded in a TG3/TR-39, VAOC compliant facility in Seal Beach, CA USA. Encryption Key loading does not occur offshore or in other facilities, so you know how secure your keys are at all times.

Magensa, LLC is the software and services subsidiary of MagTek, housed at the same facility. 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. Magensa's services and solutions are trusted by commercial, retail, financial and government enterprises without compromise.

MagTek secure transaction acceptance devices, when combined with the full suite of Magensa Managed Security Services, result in a complete end-to-end secure payment solution.

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

MagTek Hardware and Certified Products

Product Lines

MagTek manufactures a wide array of secure payment devices for many popular operating systems and interface options. MagTek products include OEM components, encrypting check scanners, secure magstripe and EMV chip readers, card issuing systems and PIN encrypting devices.

Pathway to EMV

Magensa Gateway Services currently processes magnetic stripe transactions to every major acquirer/processor and process EMV transactions through most major processors and/or direct to the major brands.

Countertop and Mobile PIN PED

MagTek's PIN Encrypting Devices (PEDs) are versatile secure cryptographic devices (SCD) and are ideal for credit, ATM, Prepaid, gift, and debit cards for traditional or mobile point of sale applications where users need unmatched convenience and security.

DynaPro is a sleek, multifunction countertop terminal that combines a PCI PTS 3.x, SRED compliant PIN Entry Device with a MagneSafe secure card reader authenticator (SCRA) and an EMV contact/contactless smart card reader with NFC capabilities. DynaPro provides all of this functionality within a slim, stylish, and rugged payment secure cryptographic device (SCD) that can be hand-held or countertop mounted.

DynaPro Go is a handheld mobile PED with magnetic stripe, EMV contact/contactless smart card reader and NFC capabilities. DynaPro Go enables card-present reading and secure manual entry of sensitive card data for card-not-present transactions.

Countertop and Mobile Secure Card Reader Authenticators

eDynamo delivers the flexibility needed to securely accept a variety of payment card technologies. Whether accepting a traditional magstripe or contact EMV card, eDynamo gives merchants the ability to connect via USB or wireless connection, offering one reader for mobile or fixed needs.

MagTek Hardware Families

MagTek and Magensa work together with the various families of hardware products to garner proper compliance and necessary certifications. The newest line of MagTek hardware is classified into three main hardware families. These families have differing levels of certifications.

- **Dynamo Family includes:** eDynamo, tDynamo, mDynamo, oDynamo, DynaWave, iDynamo 6, and DynaFlex Family Products
- **DynaPro includes:** DynaPro Go
- **SCRA Family includes:** iDynamo 5 (Gen II), Dynamag, and DynaPAD

Magensa Payment Protection Gateway (MPPG) and Magensa Decrypt and Forward (DaF) Services enable secure payment processes with a variety of L3 certified processors. One integration with Magensa provides tremendous flexibility to ISVs, VARs, ISOs, and system integrators in terms of product solutions and processor options. All of our L3 certifications include our QwickDIP (Qwickchip) technology, which improves transaction speeds and reduces complexity.

Magensa Services

Magensa Device Management

Magensa provides a repository of device configuration and activity. DynaPro devices can be shipped from MagTek in a non-active state. Upon first communication with Magensa or by instruction from the Merchant, the DynaPro devices may be activated, which puts them in a state ready to process transactions. If a Merchant needs or wants to deactivate a unit Magensa personnel can log onto a Magensa web portal and deactivate one or more units. Likewise, if a unit is to be returned to service the Merchant can instruct Magensa to reactivate the unit. In a deactivated state, Magensa will refuse to process any transactions that originate from a deactivated device.

Magensa can provide routine reports by email detailing the units in service, units out of service, together with transaction counts, and last transaction date. Ad hoc reports are also available.

One can also add address information such as store, lane, and terminal locations. On a routine basis the DynaPro devices may be polled and mutually authenticated by a cryptographic challenge response process. This aids in the detection of substituted or altered DynaPro devices and can pinpoint missing or non-working devices.

Magensa Card Authentication Service

Magensa is home to the largest globally accessible counterfeit card detection database. When a card is first seen by Magensa, its index and its MagnePrint® (a nano-particle magnetic fingerprint) are logged. When the card is next seen, Magensa notes its MagnePrint and scores it relative to the first instance. After several rounds of comparison the MagnePrint is eventually promoted to be a valid reference MagnePrint and future transactions are scored against it. If a counterfeit card is presented, the MagnePrint score drops dramatically allowing Magensa to Red-Light alert the Merchant or its service provider that fraud is about to occur.

Red-Light alerts help merchants identify counterfeit card usage that would likely pass issuer authorization, empowering them to decline the transaction before the fraud happens and therefore reduce overall chargeback exposure.

Green-Light alerts ensure the card is authentic. In fact, if the card is deemed authentic and fraud occurs, and the transaction is within MagTek scope, MagTek will absorb the financial loss due to the fraudulent transaction. MagTek scope includes, but is not limited to: the card has been registered by Magensa Services, it received a passing score, it is actually counterfeit or the relying data has been altered, and Magensa Card Authentication Services are in use (additional limits, terms, and conditions apply).

Magensa Services - Applications - MagneFlex Middleware

Magensa offers MagneFlex Middleware. Routing data from MagTek hardware directly to the Magensa Gateway with support for Windows, iOS, and Android operating systems. A bounded application (independent of the POS application) MagneFlex accepts data from an authenticated terminal, together with a dollar amount, and a transaction ID from the POS application, and forwards the packet to the Magensa Gateway. Data is decrypted, formated for authorization, and transmits the authorization message to the appropriate processor. MPPG then passes the response back to MagneFlex Middleware with the approval message, the dollar amount and the original transaction ID. MagneFlex then sends that data, and any Magensa Tokens, to the POS application software.

Simplified Development & Certification

MagneFlex is flexible and gives you freedom. After the elements in the system under test are certified, you can use any combination of the certified elements in almost any configuration. As long as you use the elements that were certified, the connection, (i.e. USB or Ethernet), location (i.e. LAN, PC, device), deployment model (mobile, brick-n-mortar), and vertical (store, restaurant, spa, etc.) don't effect the certification. This simplifies development and certification and allows you to determine the best ecosystem for each individual environment.

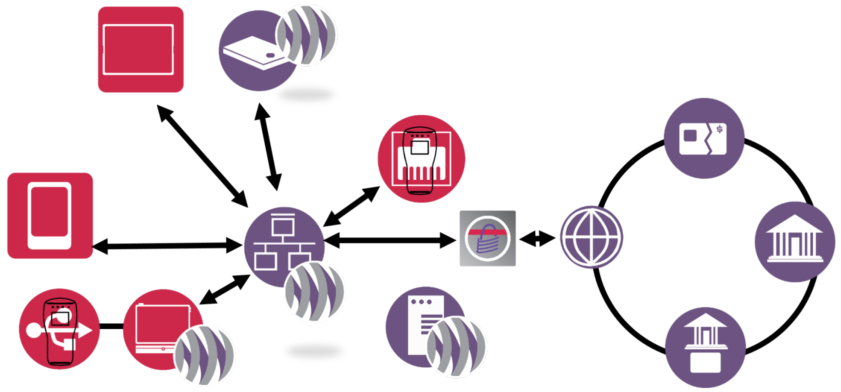


Diagram Key

POS DynaPro Terminal
Card is inserted, tapped, or swiped

USB Connection
Terminal connection type

Ethernet Connection
Terminal connection type

MagneFlex
Captures and transmits tokens and returns transaction results. Low cost and low risk routing.

POS Workstation
Loaded with or connected to MagneSafe

Local Area Network
Store LAN connection

Store Controller
Store controller with MagneFlex installed and configured

CPU per Workstation
CPU hosts MagneFlex and is directly connected and installed and configured per POS workstation

WWW
Secure Internet connection

Processor
Card processor

Brand
Card brand

Issuer
Authorized settlement

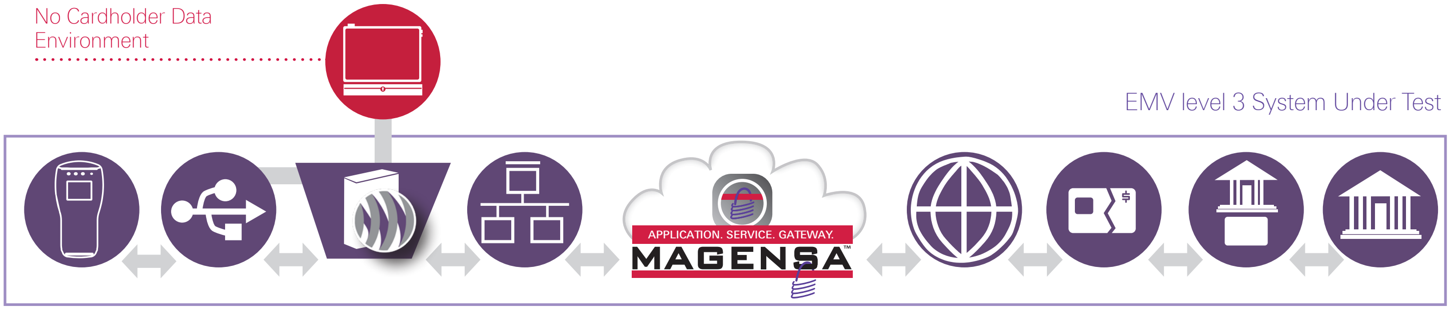
🟪 Items in Purple
EMV Level 3 System Under Test (SUT)

Magensa, LLC
Subsidiary of MagTek offering secure applications, services and gateway solutions

1 Software Semi-integrated

No additional hardware

MagneFlex is installed and configured on the local POS workstation. The POS app sends the transaction amount, type, and transaction ID to MagneFlex. In response the POS app receives APPROVE or DECLINE with the transaction amount, type and transaction ID from Magensa.

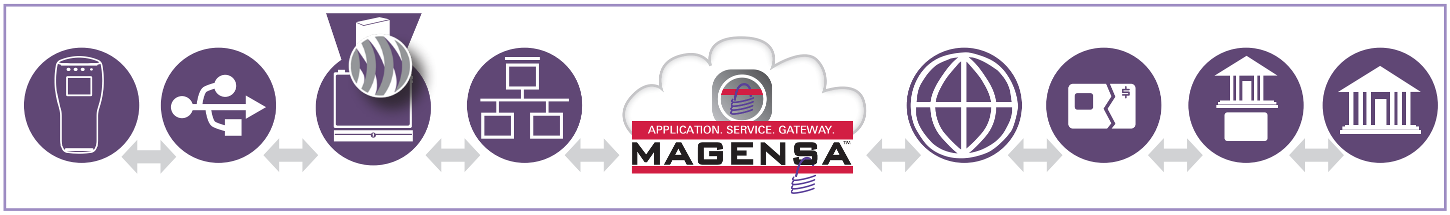

No Cardholder Data Environment
EMV level 3 System Under Test
APPLICATION. SERVICE. GATEWAY.
MAGENSA

2 Fully Integrated

No additional hardware

MagneFlex is fully integrated into the POS application.

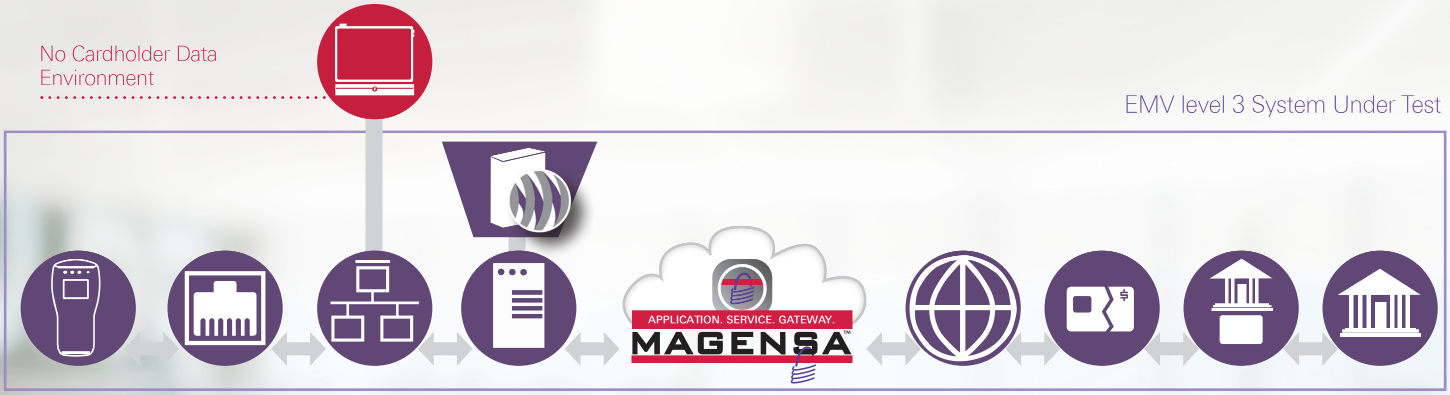
EMV level 3 System Under Test



3 Hardware Semi-Integrated

One controller is required

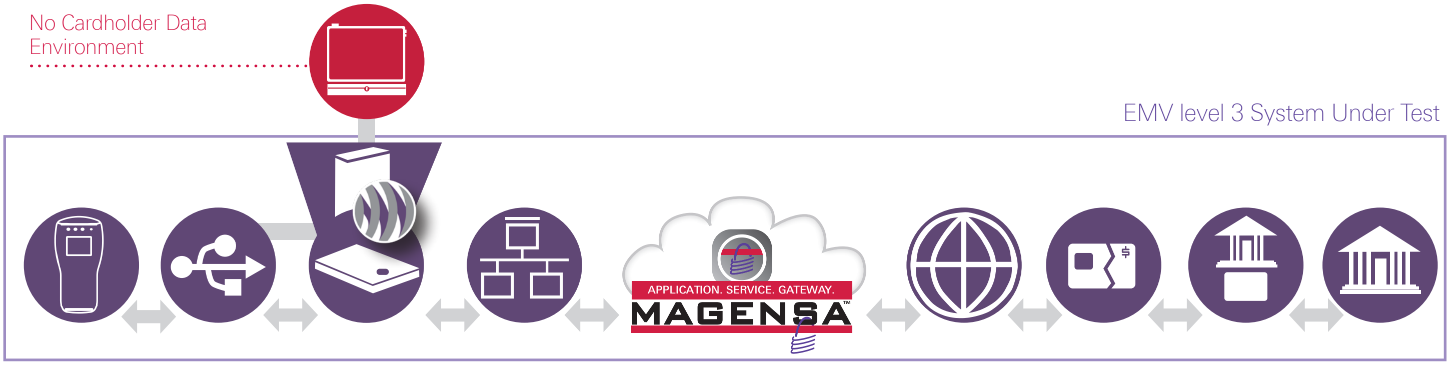
MagneFlex is centrally installed, configured and managed by a Store Controller. The POS workstations and the payment terminals all connect via Ethernet.


No Cardholder Data Environment
EMV level 3 System Under Test
APPLICATION. SERVICE. GATEWAY.
MAGENSA™

4 Hardware Semi-Integrated

One CPU per POS workstation is required

Each POS workstation and its payment terminal has its own dedicated CPU with MagneFlex installed and configured.


No Cardholder Data Environment
EMV level 3 System Under Test
APPLICATION. SERVICE. GATEWAY.
MAGENSA™

Magensa Decryption

Magensa employs HSMs (Hardware Security Modules) that safely store BDKs (Base Derivation Keys) in a FIPS (Federal Information Processing Standards) certified enclosure. No decryption is performed in software.

The HSMs are maintained in an access controlled, 24/7/365 monitored safe room within PCI DSS Level 1 certified facilities. When Magensa decrypts cardholder data or other sensitive authentication data, it does so only in the HSMs. The BDK that does the decryption never exists in DynaPro hardware, it is only resident in the HSM.

If a Merchant or its intermediary (like a Software Solution Provider) has no knowledge of or access to the keys, then the Merchant and intermediary can truthfully assert they have NO access to the clear text cardholder data or any sensitive authentication data, effectively removing them from responsibility for protection of the data and shrinking the scope of a PCI audit to the smallest possible CDE (Cardholder Data Environment).

When Merchants subscribe to Magensa's decryption services they can be assured that cardholder data entrusted to Magensa has the strongest protection available today because NIST approved algorithms and Visa originated DUKPT (Derived-Unique-Key-Per-Transaction) key management standards combine to make each transaction message a one-time, unintelligible, undecipherable blob, useless to an adversary.

Magensa Tokenization

In concert with the MagTek devices, Magensa provides multiple tokens to a Merchant or its service provider, to meet various business needs.

1) CRM Tokens

This is a non-sensitive token that can be used to provide courtesy greetings, rewards and loyalty programs, product preferences, channel choices, and store habits.
It consists of the first two and last four digits of the PAN, the Cardholder first and last name, and the card's expiry date. With this token one can greet a returning customer by name, suggest her favorite item, and notify her of an approaching award level.

2) Transaction Tokens

For each and every transaction Magensa returns a unique transaction token that can be used to look up a transaction and/or process voids or refunds without having to request or enter cardholder data.

3) Fraud Analysis Tokens

This static token allows the fraud and risk management teams to track card activity without having to know or access the clear text PAN. It is a non-reversible token.

4) Card on File Tokens

This dynamic token is returned for transactions that will likely recur in the future. After decryption of the card data at Magensa, the HSM generates a new token representing the PAN and expire date. It can be stored by the Merchant and used to process a subsequent transaction. Once redeemed, it cannot be reused. However a derivative token will be generated at Magensa and returned to the Merchant for the next instance of a recurring transaction or a transaction that takes place with multiple shipments or secondary operations.

Magensa Remote Key and Configuration Loading Services

MagTek devices were designed from the ground up to accept and authenticate replacement keys, firmware, and configuration changes at non-factory locations using Magensa remote services. To access remote services the terminals need a USB connection, and a PC with Internet Connection. To make updates even easier, MagTek has developed one-click applications that deliver secure access granted through credentials, and/or multi-factor authentication. When a secure session is established with the terminal, Magensa will send signed scripts to update the device and then update the device management database. The terminal will validate the intention of the new data and will permit only authenticated updates. Magensa is then updated of its success or other status.

Magensa Multi-Factor Authentication Services

Magensa supplies Qwantum counterfeit resistant access cards that serve as part of the permission process for sensitive transactions. Qwantum cards generate unique, unpredictable, one-time use tokens, which when authenticated, can allow access to activities like changing software, passwords, configurations and permitting remote access to the Merchant's POS system. Because the cards cannot be cloned and tampering with the encoded data can easily be detected, their use buttresses a multi-factor approach to security. Qwantum cards used as a token generator is easier, safer and less expensive than a token display fob. It does not rely on a real-time clock but does generate a very large token with an enormous entropy factor, yet there's nothing the user must read or type.

Magensa Gateway Services

Magensa's Gateway Services are cost-effective and easy to use. Integration time is minimal and MagTek offers a wide variety of development tools to easily integrate a wide array of MagTek devices across multiple platforms and operating systems.

- Magensa Decrypt and Forward Gateway
- Magensa Payment Protection Gateway (MPPG)
- Magensa Tokenization Service can be combined with Decrypt and Forward or MPPG
- Magensa Tokenization as a Service

Magensa Payment Protection Gateway Service (MPPG) works as your secure rail to send encrypted data onto processors, gateways, and acquirers and to return the authorization. The POS app sends encrypted data to Magensa to perform authorization, sale, void, refund, capture, and magnetic stripe card and device authentication. Magensa decrypts the data and bundles it with Magensa's APIs and sends out for processing. Magensa returns the authorization and magstripe card and device authentication. This delivers a simplified platform for decryption and gateway services for VARs and ISOs.

Developer Toolkit and Key Injection

P2PE Toolkit

In order to obtain a PCI P2PE certification by a qualified P2PE assessor many things are required, including a fully documented system. The combination of MagTek hardware and Magensa Managed Security Services can assure rapid attainment of a P2PE certification.

Key Injection

Key injection is performed securely at MagTek or in the field. MagTek's Key Injection Facility (KIF) and Magensa's Remote Key Injection (RKI) services are both in compliance with the TR-39/ PCI PIN requirements, and are frequently re-validated for compliance via external audits. Device Estate Management performed by Magensa includes deployment monitoring, activation, deactivation, destruction, and reporting tools.

All decryption takes place outside the Merchant and/or Service Providers' environment in a PCI Level 1 certified facility. No keys are shared with the Merchant or Service Provider.

No cardholder PANs or sensitive authentication data whether, swiped, dipped, tapped, or hand keyed is exposed or available to the Merchant or its Service Providers. Magensa enforces Two Factor authentication for high risk transactions. The CDE (Cardholder Data Environment) is as small as possible.

Magensa Managed Security Services, coupled with MagTek's devices, provide a comprehensive, layered, end-to-end protected payment security solution at a reasonable cost. Engineered to be rugged, flexible and secure MagTek and Magensa deliver a solution that is scalable, defensible, and offers a rapid pathway to P2PE and EMV certifications.

MAGENSA™
SIMPLY STOPS FRAUD

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. Magensa's services and solutions are trusted by commercial, retail, financial and government enterprises without compromise. Magensa, LLC is a subsidiary of MagTek, Inc.